الجمهورية الجزائريةالديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة قاصدي مرباح – ورقلة

كلية الرياضيات و علوم المادة

قسم الفيزياء

مذكرة تخرج مقدمة لنيل شهادة

ماستر أكاديمي

مجال: علوم المادة

تخصص: فيزياء إشعاعية

من إعداد الطالبتين : حسيني أسماء – بوقفة سليمة

الموضوع

الحاسوب الكمومي

(بحث خوارزمية Grover)

نوقشت يوم : 2018/06/04.

أمام لجنة المناقشة المكونة من الأساتذة :

بن بيتور عبد الوهاب	أستاذ محاضر (أ)	جامعة قاصدي مرباح – ورقلة	مشرفا
خلفاوي فتحي	أستاذ التعليم العالي	جامعة قاصدي مرباح –ورقلة	رئيسا
قربوسة ياسين	أستاذ محاضر (ب)	جامعة قاصدي مرباح ورقلة	مناقشا

الموسم الجامعي : 2018/2017.

الملخص:

الحاسوب الكلاسيكي هو خوارزمية تحول بتات مخزنة على شكل نظام ثنائي (1،0) إلى نتائج كذلك على شكل بتات. أما الحاسوب الكمومي هو خوارزمية تعتمد على النظم الكمية لتحويل بتات كمومية إلى نتائج على شكل بتات كمومية يتم قياسها لقراءة النتائج. الخوارزميات الكمومية تختزل العمليات الكلاسيكية لأنها تعتمد على الظواهر الكمومية من التداخل والتشابك من أهم هذه الخوارزميات هي خوارزمية Grover التي تسمح بفصل المعطيات حسب معيار معين تفوق بطريقة أسية الخوارزميات الكلاسيكية. تناولت هذه المذكرة موضوع الحاسوب الكمومي، فحددت الخوارزميات التي تصف عمل الحاسوب الكمي إضافة إلى Grover تطرقنا لخوارزمية Simon وخوارزمية Deutsch–Jozsa، وتم فيها القيام بالعمليات والبوابات الكمومية، أين تم التعرض للتشابك الكمي، ومن تطبيقاته تعرضنا لنظرية عدم الاستنساخ والنقل الكمي والترميز المكثف وتوزيع المفتاح الكمومي.

الكلمات المفتاحية : التشابك،التراكب، الكمبيوتر الكمي، البت الكمي(qubit)، خوارزمية، البوابات الكمومية

Abstract :

The classical computer is an algorithm that transforms bits stored in a binary form into results that are like wise bits. Similarly, the quantum computer is an algorithm based on quantum laws, which transforms qubits into other yielding the aleshed results after measuring. Quantum algorithms reduce the classic operations because of the phenomen of entanglement and interference. One important example is Grover's algorithm,allows separating elates (according to some criterion) in a time exponentially less than that of the classic algorithms. This dissertation treats the above subject. We focus on some examples that exemplify hour a quantum computer might work. The main algorithms treated here are the ones clue to Grover, Simon, Deutch-Jozsa. As an application we touched on the theory" no-Cloning Theorem", "quantum teleportation" and 'dense cryptography' and 'Quantum KeyDistribution'.

Key words: Entanglement, interference, quantum computer, qubit, algorithm, quantum gates.

الإهـــــــداء

يصعب علي أن أفيكما حقكما . . . لكما أهدي هذا العمل

أمي وأبي أطال الله في عمرهما

إلى إخوتي وأخواتي

إلى كل رفيقاتي

إلى كل من ساعدني من قريب أو بعيد لإتمام هذا العمل

شـــكر وتقديـــــر

بعد باسم الله الرحمان الرحيم

الحمد أولا ودائما على جميل إحسانه وحسن توفيقه لي في إنجاز هذا العمل

المتواضع، الذي أرجو أن يكون مقبولا عنده ،فلك الحمد ربي حتى ترضى

ولك الحمد إذا رضيت ولك الحمد على نعمة الحمد.

لا يسعني في هذا المقام، وكل مقام، إلا أن أتقدم بجزيل الشكر

والامتنان وأسمى عبارات التقدير إلى من علمني وأنار لي درب العلم والمعرفة

وقدم الكثير والكثير دون كلل أو ملل، الأستاذ المشرف : ' بن بيتور عبد الوهاب '

الذي أسأل الله أن يجزيه خير الجزاء.

كما أتقدم بجزيل الشكر والامتنان للسادة : خلقاوي فتحي و ياسين قربوسة أعضاء لجنة التحكيم

ولقسم الفيزياء بجامعة قاصدي مرباح ،لكل من ساعدني وأرشدني

ولكل من قدم لي يد العون ولو بكلمة طيبة.

الفهرس

فهرس الأشكال

فهرس الجداول

المقدمة العامة

المقدمة العامة

ليس غريبا على ميكانيك الكم أن تتفرد بظواهر غريبة ولا أن تختص بمزايا فريدة، وهي التي ما فتئت تتعرض للانتقادات وتساق نحوها المتناقضات لتعارضها مع العديد من الأفكار الموجودة والمسلمات المفروغ منها في العالم الكلاسيكي، ونجحت رغم ذلك في الصمود حتى اليوم لقدرتها على تفسير ظواهر العالم الكمي وتناسق توقعاتها مع النتائج التجريبية في العالم الحقيقي. الحاسوب الكمي هو من أحدث الاستعمالات المرتقبة للظواهر الكمومية كما أستعملت من قبل في صناعة المركبات الاكترونية والليزر و غيرها.

كانت بدايات الحوسبة الالكترونية مع آلان تورينج عالم الرياضيات عام 1936 حين طور جهاز كمبيوتر قابل للبرمجة وهو نموذج للحسابة المعروفة باسم آلة تورينج، لم يمض وقت طويل بعد اكتشاف تورينج شيدت أول أجهزة الكمبيوتر من المكونات الالكترونية، نمت أجهزة الكمبيوتر بوتيرة مذهلة لدرجة أن النمو قد تم تقنينه من قبل غوردون مور عام 1965 المعروف باسم قانون مور الذي ينص على أن قوة الكمبيوتر سوف تتضاعف بتكلفة ثابتة تقريبا مرة كل سنتين..

قد يفشل قانون مور في نهاية المطاف عند الإنتقال إلى نموذج حوسبة مختلف. وتقدم واحد من هذه النماذج من قبل نظرية الحاسب الكمومي، والتي تقوم على فكرة استخدام ميكانيك الكم لأداء الحسابات بدلا من الفيزياء الكلاسيكية. اتضح أنه في حين الكمبيوتر العادي يمكن أن يستخدم محاكاة كمبيوتر الكمومي لكن أنه من المستحيل أداء محاكاة بطريقة فعالة، وبالتالي أجهزة الكمبيوتر الكمي توفر أساسية ميزة السرعة على أجهزة الكمبيوتر الكلاسيكية. ويعتقد العديد من الباحثون انه لايمكن تصور كمية من التقدم في الحاسب الكمومي تكون قادرة على التغلب على الفجوة بين قوة الكمبيوتر الكلاسيكي وقوة الكمبيوتر الكمومي[1] .

جاء عام 1995 عندما أظهر لوف غروفر مشكلة إجراء بحث من خلال بعض مساحة البحث غير مهيكلة، تقدم خوارزمية غروفر تطبيق واسع النطاق للمنهجيات القائمة على البحث تكون أسرع على كمبيوتر الكم. اقترح ريتشارد فينمان في عام 1982 فكرة أشار أنه يبدو هناك صعوبات أساسية في محاكاة نظم الكم الميكانيكية على أجهزة الكمبيوتر الكلاسيكية، واقترح أن بناء أجهزة الكمبيوتر على أساس مبادئ ميكانيك الكم التي تسمح بتجنب تلك الصعوبات. وعام 1990 بدأت تجسيد فكرة استخدام محاكاة الكمبيوتر الكمي [1].

حاسوب الكم هو جهاز يستخدم الظواهر والنظم الميكانيكية الكمية لإجراء العمليات الحسابية والتعامل مع البيانات ودراسة معالجة المعلومات والمهام، ويجسم سلوك الجسيمات في المستوى تحت الذري، مثل التشابك والتراكب ويعتمد على كيوبت والذي هو (إما 0 أو 1 أو كلاهما).ويستعمل الحاسب الكمومي من أجل خوارزميات أكثر كفاءة متوازية، التشفير الكمي (خرق الشفرات وتأمين البيانات)، محاكاة النظم الكمومية[2][1] .

تعمل الحواسيب الكمومية بشكل مشابه لآلة تورينج ويتم ذلك عبر التلاعب بالبتات الموجودة في إحدى الحالتين (0 أو 1) فهي تشفر البيانات داخل بتات كمومية التي تستطيع التواجد في حالة تراكب، حيث تمثل البتات الكمومية : الذرات، الأيونات، الفوتونات، الإلكترونات وأجهزة التحكم الخاصة بها والتي تعمل كلها معا كذاكرة حاسب ومعالج[3] .

وهذا التراكب الحاصل في البتات الكمومية هو ما يقدم للحواسيب الكمومية توازيها، الذي يسمح للحاسوب الكمومي بالعمل على إجراء مليون عملية حسابية في نفس اللحظة بالمقابل يقوم الكمبيوتر العادي بعملية واحدة فقط [3].

يمكن للجسيمات أن تتصرف مثل الموجات إذ أنها يمكن أن تتواجد في صورة جسيمات أو موجة أو جسيم وموجة معا، ونتيجة لهذا التراكب نسمي البت بالكيوبت[4] .

العمل الحالي يهدف لتقديم القالب الرياضي والفيزيائي للحاسوب الكمي، مع الإحاطة بالموضوع من جميع جوانبه بشكل متكامل قدر الامكان، هذا بالإضافة إلى التعزيز بالأمثلة و بالبرهان.

الفصل الأول يقدم بعض الجوانب الرئيسية لميكانيك الكم، وأهم التعريفات في الحاسوب الكمومي، مع لمحة عمل الحاسوب الكلاسيكي.

الفصل الثاني تطرقنا إلى التعرف على أهم بوابات المنطق الكمومي و يحدد العدة الرياضية اللازمة للأنظمة والظواهر الكمومية (تراكب وتشابك)، كما عرفنا مفهوم التشابك الكمي وتطرقنا إلى أهم تطبيقاته المستخدمة في الحوسبة الكمومية.

الفصل الأخير تتم فيه عملية تطبيق لخوارزمية GROVER كمثال لدراسة الحاسوب الكمومي مع ذكر بعض الخوارزميات المهمة في برمجة الحوسبة الكمومية .

وعموما الموضوع حديث و لازال قيد البحث لحد اليوم.

الفصـــــل الأول

بعض الجوانب الرئيسية في ميكانيك الكم وأهم التعريفات في الحاسوب الكمومي

1.I.تمهيد

إن دراسة سلوك العالم الذري يعتمد بشكل كامل على ما تتوقعه ميكانيك الكم، فهي النظرية الوحيدة القادرة على التنبؤ بهذا السلوك، و ذلك من خلال مجموعة من المسلمات والمبادئ الفيزيائية الأساسية .

2.I.المبادئ الأساسية في الفيزياء الكمومية[1].*(Nielsen and Chuang.)*

المبدأ الأول :تعريف للبيت الكمي أو للكيوبت .

المبدأ الثاني :تطور حالة القياس .

المبدأ الثالث : مبدأ القياس .

المبدأ الرابع :مزج الكيوبيتات.

I-2-1-المسلمة الأولى :

تعرف الحالة الكمومية لجملة الفيزيائية بمتجه في فضاء شعاعي مركب (فضاء الحالات) له هيكل فضاء هلبرتي. ضمن هذه المذكرة نعتبر الجمل الكمومية ذات الحالتين الأساسيتين و يكون فضاء الحالات فضاء هلبرت يذو بعدين أساسه$|1\rangle$ و $|0\rangle$(الحالتين الأساسيتين) و مزود بجداء سلمي فتصبح حالة الجملة هي في العموم مزج خطي للحالتين الأساسيتين

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (1.I)$$

نختار دوما حالة الجملة نظامية $|\alpha|^2 + |\beta|^2 = 1$.

a. **تعريف ال *QBIT***

نعرف ال qbit على أنه أي جملة كمومية ذات حالتين أساسيتين فيصبح حالة ال qbit معرفة بالمزج الخطي $\alpha|0\rangle + \beta|1\rangle$ مع شرط التنظيم : $|\alpha|^2 + |\beta|^2 = 1$

I-2-2-المسلمة الثانية :تطور حالة *qubit*

تطور الحالات في نظام الكم يوصف بالتحويل الوحدوي وهذا يعني أن الحالة $|\psi(t)\rangle$ للنظام في الزمن t مرتبطة بالحالة $|\psi(t')\rangle$ للنظام في الزمن t' بواسطة التحويل الوحدوي U

$$|\psi(t')\rangle = U(t',t)|\psi(t)\rangle$$

مع: $U^{\dagger}U = 1$

ملاحظة:هذا التحويل يحوي العمليات التي نستطيع إجراءها على حالات كيوبيت .

مثال 1:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

$$|\psi'\rangle = U|\psi\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$$

مثال 2:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

$$U = \sigma_z = Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

$$|\psi'\rangle = U|\psi\rangle = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\left(\alpha|0\rangle + \beta|1\rangle\right) = \alpha|0\rangle - \beta|1\rangle$$

I-2-3-المسلمة الثالثة : مبدأ القياس

القياس هو التحول الوحيد الذي يغير من حالة الكيوبت بطريقة غير وحدوية .

يتم وصف القياسات الكمية بواسطة مجموعة $\{M_m\}$ من مؤثرات القياس , هذه المؤثرات التي تؤثر على حالة المكان للنظام الذي يتم قياسه .

يشير المؤشر m إلى نتائج القياس التي قد تحدث في التجربة .

إذاً حالة النظام الكمومي هي $|\psi\rangle$ قبل القياس مباشرة, ثم الإحتمال الذي ينتج عن m يحدث بواسطة

$$P(M) = \langle\psi|M^{\dagger}{}_m M_m|\psi\rangle \qquad (2.I)$$

وحالة النظام بعد القياس

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M^{\dagger}{}_m M_m|\psi\rangle}} \qquad (3.I)$$

تستجيب مؤثرات القياس لمعادلة الاكتمال

$$\sum_m M^{\dagger}_m M_m = I \qquad (4.I)$$

وتعبر معادلة الاكتمال عن حقيقة أن الاحتمالات تصل إلى واحد

$$1 = \Sigma_m P(m) = \Sigma_m \langle\psi|M^{\dagger}{}_m M_m|\psi\rangle \qquad (5.I)$$

هذا هو القياس على qbit واحد مع اثنين من النتائج محددة بواسطة مؤثر القياس

$|M_0 = \langle 0|0\rangle$ و $M_1 = \langle 1|1\rangle$

$$M_1 = \binom{0}{1}(0,1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad M_0 = \binom{1}{0}(1,0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

نلاحظ ان كل عامل قياس هو Hermitian، وهذا

$$M_0{}^2 = M_0 \;\; ; \;\; M_1{}^2 = M_1$$

وبالتالي علاقة اكتمالها تعطى $I= M^{\dagger}{}_0M_0 + M^{\dagger}{}_1M_1 = M_0 + M_1$

نفترض الجملةψ في حالة $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ثم احتمال الحصول على القياس النتيجة 0 هي

$$P(0) = \langle\psi|M^{\dagger}{}_0M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = \quad |\alpha|^2 \qquad (6.I)$$

وبالمثل ، فإن احتمال الحصول على نتائج القياس 1 هي$P(1) =|b|^2$. الحالة بعد القياس في الحاتين هي[1]

$$\frac{M_0|\psi\rangle}{|\alpha|} = \frac{\alpha}{|\alpha|}|0\rangle \qquad (7.I)$$

$$\frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle \qquad (8.I)$$

I-2-4-المسلمة الرابعة : n −qbit

مزج الكيوبيتات (الجداء التنسوري)

فضاء الحالة للنظام المادي المركب هو الجداء التنسوري لفضاءات الحالة للنظم المادية المكونة

نعتبر الأنظمة 1 عبر n والنظام i في الحالة $|\psi_i\rangle$ الحالة المشتركة للنظام الكلي [1]

$|\psi_1\rangle\otimes|\psi_2\rangle\otimes|\psi_3\rangle\otimes \dots\dots\otimes|\psi_n\rangle$ الناتجة من $H_1\otimes H_2\otimes H_3\otimes H_4\otimes \dots\dots\otimes H_n$

مثال :ليكن النظام الكلي مكون من حالتين لنظامين

حالة الجملة $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ تنتمي إلى الفضاء الهلبرتي H_1

وحالة الجملة $|\psi_2\rangle = \delta|0\rangle + \lambda|1\rangle$ تنتمي الى الفضاء الهلبرتي H_2

حالة النظام $|\psi\rangle \in H_1 \otimes H_2$

$\otimes$ يسمى جداء تنسوري

I.3.الحالة الكوانتية *(up ;down)*

نرمز للحالتين الكوانتيتين ببناء بتات كمومية $|0\rangle = |\uparrow\rangle_z \; ; \quad |1\rangle = |\downarrow\rangle_z$

الحالة ***up:***

$$|\uparrow\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad (9.I)$$

الحالة ***down :***

$$|\downarrow\rangle_x = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) \qquad (10.I)$$

I.4.البت الكمي*(qubit)*

البِت الكمي هو وحدة المعلومات الكمية أي الوحدة الأساسية للمعلومات في الكمبيوتر الكمي، نظيره في نظرية المعلومات الكلاسيكية هو البِت(bit) والذي يمكن أن يأخذ فقط أحد القيمتين {0،1}، أما البِت الكمي و نتيجة لمبدأ التراكب في ميكانيك الكم فيمكن أن يكون في شكل أي تركيبة خطية من الحالتين السابقتين:

$$\alpha|0\rangle + \beta|1\rangle \qquad (11.I)$$

أين وهما عددان مركبان. البت الكمي إذ هوأبسط نظام كمي ممكن، بعد فضائه هو اثنان وأساسه هو {$|0\rangle$ ،$|1\rangle$} غالبا ما يعامل البِت الكمي رياضيا دون العودة الحقيقة الفيزيائية، ذلك أنه يمكن أن يسقط

على العديد من الأنظمة الفيزيائية مثل: ذرات أو أيونات ذات مستويا طاقة، جسيمات ذات سبين، 1/2 استقطاب فوتون وحيد وغيرها[3,2].

نستخدم تدوين ديراك($|bra\rangle\langle Ket|$) ، وحالة التراكب لنظام الفيزياء ، وعلى وجه التحديد الأنظمة التي لديها نظام محتمل مثل نظام الاستقطاب ، والأنظمة ذات السبين...

يمكن أن تكون حالة النظام ممثلة بالحالة $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ حيث $\alpha, \beta \in \mathbb{C}$ حيث نحتاج إلى أن تكون هذه الحالة منظمة .

$$|\alpha|^2 + |\beta|^2 = 1 \qquad (12.I)$$

'bit 'هي اختصار لكلمة'digit Binary '

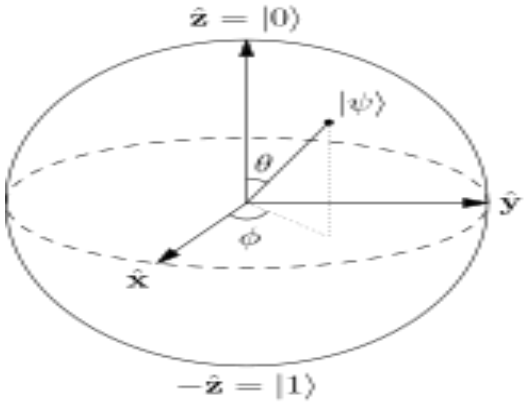
هذا يسمىqubit، يمكن أن تمثل متجه حيث $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi\rangle = \alpha\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

كما يمكننا أن نمثلاثنين منqubitعلى النحو التالي

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \rightarrow \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix}$$

في مزيد من التعميم، تمثيلn-qubitمن قبل



الرسم التخطيطي(I.1): كرة بلوخ

$$|\psi\rangle = \alpha_{00...0}|00...0\rangle + \alpha_{00...1}|00...1\rangle + ... + \alpha_{11...1}|11...1\rangle = \sum_{i=0}^{n} \alpha_i |x\rangle \quad (13.I)$$

أين $|ab\rangle$ هو متجه الأساس الذي يمثل حالة حيث تكون qubit الأول في الحالة $|a\rangle$ و qubit الثاني في الحالة $|b\rangle$ وهكذا.

و $\alpha_i \equiv \alpha_{00...0}, \alpha_{00...1}, ..., \alpha_{11...1}$ أين $\sum(\alpha_i)^2 = 1$ و $|x\rangle$ هو متجه التحيز.

وتمثل كل حالة أساسية ناقلاً في مجال بلوخ (Bloch sphere) ؛ وهو تمثيل هندسي لنظام كمي ذي مستويين يتم تقديمه ، بحيث يكون معامل $|0\rangle$ (ket) هوحقيقيًا غير سلبي .باستخدام هذا وقيد التنظيم، من المفيد عدم استخدامαوβ، ولكن بدلاً من ذلك استخدام:

$$\alpha = \cos\left(\theta/2\right) \text{ and } \beta = e^{i\phi}\sin\left(\theta/2\right), \text{ where } 0 < \theta < \pi \text{ and } 0 < \phi < 2\pi$$

عندما نستخدم هذا الترميز، فإنه يمنحنا إمكانية تمثيل كل ناقلات الأساس qubit (أحادي) في كرة تسمى كرة بلوخ.[4]

في الكمبيوتر الكلاسيكي , أصغر وحدة من DATA هي بت ، عنصر مجموعة عنصرين $\{0,1\}$ ، في الحساب الكمومي أصغر وحدة من DATA هي بت كمي أو qubit ، تُعرَّف على أنها شعاع في فضاء هيلبرت أوكرة بلوخ .

I.5.اثنين من البت الكمي (*Qubit*)

في الحوسبة الكمومية فإن qubit واحد لا يكفي لإجراء حساب عام ، لتصحيح هذا نضيف qubit الثاني. لنفترض أن لدينا نظام2 qubit ، كل qubit في حالة تنتمي إلى مجموعة من عدد معقد $\mathbb{C}^2$، وبالتالي فإن الحالة العامة للنظام الجداء التنسوري لاثنين من كوبيت $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$.

المتجهات هي تقصير على التوالي $|00\rangle,|01\rangle,|10\rangle,|11\rangle$

$$|01\rangle \otimes |01\rangle = |0001\rangle, |10\rangle \otimes |01\rangle = |0010\rangle, |01\rangle \otimes |10\rangle = |0100\rangle, |10\rangle \otimes |10\rangle = |1000\rangle \quad \textbf{(I}14.)$$

I.6.العديد من البت الكمي(*n-qubit)*

لمزيد من التعميم،يحتوى نظام الكم على n حالة، وحالة كل النظام هوالجداء التنسوري ل n−qubit

n−qubitهي متجه في فضاء

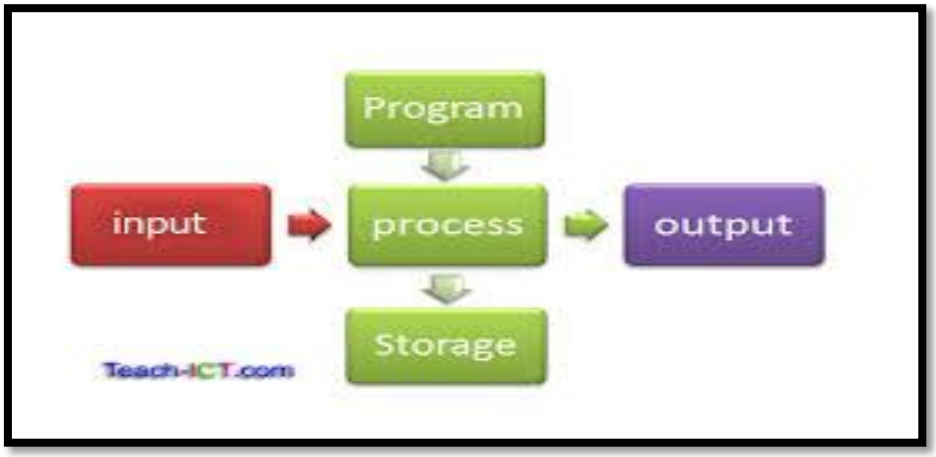
$$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n} \qquad (15 .I)$$

مثال :n=3 اذن $\mathbb{C}^8 \ni$الاتجاه

$$|000\rangle,|001\rangle,|010\rangle,|011\rangle|100\rangle|101\rangle|110\rangle|111\rangle$$

I.7.الخوارزمية الكلاسيكية:

I..17. تعريف الخوارزمية:هي مجموعة من الخطوات المنطقية لحل مشكلة، في "خوارزمية" الرياضيات تعني:



الرسم التخطيطي(2.I):تخطيط يوضح بنية الخوارزمية

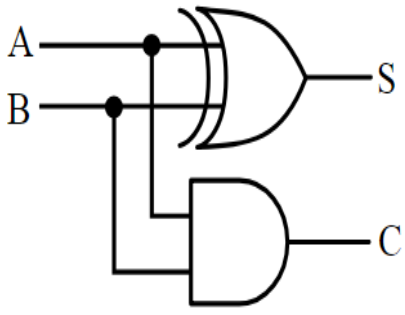
وعادت خوارزمية الاسم إلى عالم الرياضيات المسلم "أبو جعفر محمد ابن موسى الخوارزمي"،

2.7.I.المنطق الرقمي:

جميع الآلات الرقمية، تستند إلى مبدأ بسيط، هو تمثيل للمعلومات بأرقام السحب {0 و 1}، حيث تتكون كل آلة من مجموعة من الدوائر الإلكترونية. كل دائرة توفر وظيفة منطقية محددة (إضافة ، مقارنة).

مثال

شبكة جمع بين Aو B



A	B	S	C
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

C هي الاحتفاظ

S هي الجمع

الخوارزمية :

المدخلات: $A, B \rightarrow (0,0);\ (0,1)\ ;(1,0);\ (1,1)$

$$s = \bar{A}\, B + A\bar{B}$$

$$C = A.B$$

أظهر النتيجة:المخرجات

8.I.الجبر البولي :

1.8.I. الملخص:

لتصميم وتحقيق دوائر الإلكترونيات ، يجب أن يكون لدينا نموذج رياضي للوظيفة التي تحققها هذه الدائرة ، يجب أن يأخذ هذا النموذج بعين الاعتبار النظام الثنائي.

جورج بوول هو عالم رياضيات إنجليزي (1815–1864) ، وقد قام بعمل أعمال تتشكل وظائفها (تعبيرات) من خلال المتغيرات التي يمكن أن تأخذ القيم "نعم" أو"لا".

النموذج الرياضي المستخدم هو "الجبر البولي".

وقد استخدمت هذه الأعمال لدراسة الأنظمة التي لها حالتين متبادلتين:

يمكن أن يكون النظام في حالتي E1 و E2 فقط بحيث يكون E1 هو عكس E2.

لا يمكن أن يكون النظام في حالة E1 و E2 في نفس الوقت، يتم تكييف هذه الأعمال بشكل جيد مع النظام الثنائي (0 و1).

1.1.8 .I .النظام الثنائي (0 و 1):

الجبر البولي هو نوع مختلف من الجبر أو بالأحرى يمكن أن يقال نوع جديد من الجبر الذي اخترعه عالم الرياضيات الشهير جورج بوول في عام 1854. نشره في كتابه "تحقيق قوانين الفكر ."في وقت لاحق باستخدام هذا الأسلوب قدم كلود شانون نوعًا جديدًا من الجبر الذي يُطلق عليه "تبديل الجبر ." في الالكترونيات الرقمية هناك عدة طرق لتبسيط تصميم الدوائر المنطقية .هذا الجبر هو واحد من هذه الطرق .وفقا لرموز جورج بوول يمكن استخدامها لتمثيل هيكل الأفكار المنطقية .هذا النوع من الجبر يتعامل مع القواعد أو القوانين، والتي تعرف باسم قوانين الجبر البوولية التي تنفذ بها العمليات المنطقية.

هناك أيضًا بعض النظريات حول الجبر البوولي، والتي يجب الانتباه إليها بحذر لأن هذه العمليات تجعل الحساب أسرع وأسهل.يتعامل المنطق البوولي مع متغيرين فقط 1و 0، حيث يتم تنفيذ جميع العمليات الحسابية.

هناك ثلاث عمليات ثنائية فقطAND و OR و NOT يتم بواسطتها تنفيذ جميع العمليات الرياضية الثنائية البسيطة والمعقدة .هناك العديد من القواعد في الجبر البولي الذي يتم من خلاله القيام بهذه العمليات الحسابية . في الجبر البولي، يمثل الحرف الأول من الإنجليزية مثل B،A، C، الخ المتغيرات، ويمكن أن تكون قيمة كل متغير إما 1 أو 0، ولا شيء آخرفي الجبر البولي، يمكن أيضًا تحويل التعبير المعطى إلى رسم بياني منطقي باستخدام بوابات منطقية مختلفة مثل بوابة AND و بوابة أو بوابة NOT وبوابات NOR وبوابات NAND وبوابات XOR وبوابات XNOR إلخ.

I.8.2. بديهيات الجبرالبولي :

I.8.2.1. القانون التراكمي للجبر البولي:

$$A+B+C=A+C+B=B+A+C=B+C+A=C+A+B=C+B+Q$$
$$A.B.C=A.C.B=B.A.C=B.C.A=C.A.B=C.B.A \quad \text{(I17.)}$$

وفقا للقانون التراكمي، لا يؤدي ترتيب عمليات OR و AND العمليات التي أجريت على المتغيرات إلى أي اختلافات.

I.8.2.2. القوانين التجميعية للجبر البولي:

$$(A+B)+C=A+(B+C)$$
$$(A.B).C=A.(B.C) \quad \textbf{(18.I)}$$

يعتبر هذا القانون لعدة متغيرات، حيث تكون عملية OR لنتيجة المتغيرات متماثلة مع تجميع المتغيرات .

هذا القانون هو نفسه في حالة عملية AND .

I.8.2.3. القوانين التوزيعية للجبر البولي:

$$A.(B+C)=A.B+A.C \quad (19.I)$$

يتكون هذا القانون من اثنين من المؤثرات **AND** و **OR**

I.8.3. بعض القوانين الأساسية للجبر البولي:

$\bar{0}=1, \bar{1}=0,$ if A=1 then $\bar{A}=0,$ and if A=0, then $\bar{A}=1.$

A.0=0 حيث A يمكن أن تكون إما 0 or 1.

A .1 = A حيث A يمكن أن تكون إما 0 or 1.

A . A = A حيث A يمكن أن تكون إما 1 or 0

$A . \bar{A} = 0$ حيث A يمكن أن تكون إما 1 or 0

A+0 = A حيث A يمكن أن تكون إما 1 or 0

A+1=1 حيث A يمكن أن تكون إما 1 or 0

$A+\bar{A}=1$

A+A=A

A + B = B + A حيث A يمكن أن تكون إما 1 or 0

A . B = B. A حيث A يمكن أن تكون إما 1 or 0

قوانين الجبر البولي صحيحة أيضا لأكثر من متغيرين.

9.I.بت *(Bit)*:

1.9.I تعريف :

البت وحدة قياس للمعلومات، تُستخدم في حوسبة المعلومات والاتصالات الرقمية، في حين أن البتة الواحدة تتكون من قيمة ثنائية إما 0 أو 1، كما يمكن أن تمثل قيمة حقيقية أو خاطئة، الرقم الثنائي هو رقم يمكنه اعتماد واحدة من قيمتين ممكنتين 0 أو 1،في حين أن البتة هي الحد الأقصى لمقدار المعلومات التي يمكن نقلها من خلال رقم ثنائي.

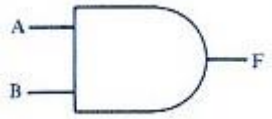
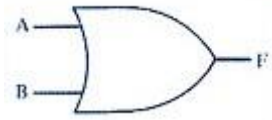
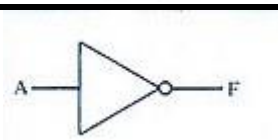
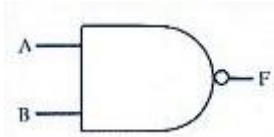
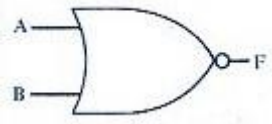
2.9.I. التمثيل الفيزيائي :

0 :يعني أنه لا يوجد إشارة كهربائية

1:وجود إشارة كهربائية

I.10.العمليات الكلاسيكية (Bit Wise Operations):

الجدول(I.1):البوابات المنطقية وتمثيل الرسومات الخاصة بهم

الإسم	مخطط الرمز	الوظيفة الجبرية
AND		$F = A + B$ *or* $F = AB$
OR		$F = A \div B$
NOT		$F = \bar{A}$ *or* $F = A'$
NAND		$F = \left(\overline{AB}\right)$
XOR		$F=\bar{a}b+a\bar{b}$
NOR		$F = \left(\overline{A+B}\right)$

أين $\bar{X}$ هو تكملة. X

الفصل الثاني

البوابات الكمومية والتشابك الكمي

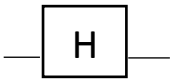
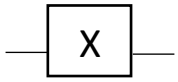
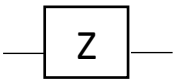
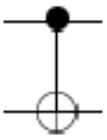
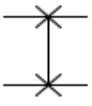
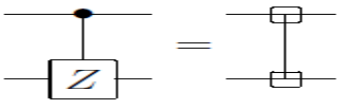
1.II.تمهيد

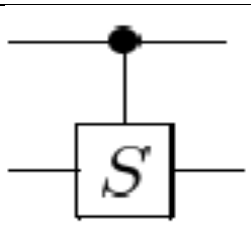
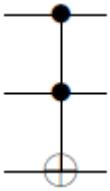
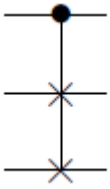
من المعروف ان البوابات الكلاسيكية عكسية لا رجعية فيها لدينا سياق أفضل لتقدير فوائد البوابات الكمومية يمكن تقسيم أي حساب كلاسيكي الى عدة بوابات كلاسيكية وذلك عن طريق سلسلة من الحساب تعتمد على نظام ثنائى (0.1) بينما البوابات المنطق الكمومي فهي تعمل فقط عدد قليل من الكوبيتات تسمح باعطاء نتائج كمومية في اقل وقت ممكن.

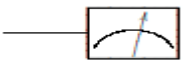
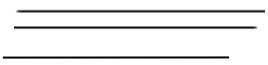
الفرق الموجود بين البوابات الكلاسيكية والكوانتية هو التلاعب في البت كلاسيكيا يكون البت (0او.1) اما الكوبت(البت الكمومي0.او 1او معا)، حالة تراكب كمومي تسمح بحساب الحالة الأساسية التي غالبا ما تكون متشابكة.

لاشك في أن التشابك الكمي يصور الغرابة التي يكتنف العالم الكمي في أكثر مظاهر جلاء ، خاصة أن هذه الخاصية الكمية ليس لها من مثيل كلاسيكي وهو ما يجعل منها موردا جديدا يمكن من خلاله تنفيذ أمور بدت سابقا مستحيلة. الأمر المثير بشأن التشابك الكمي هو السبل الجديدة التي يفتحها ، و الآفاق الممكنة لاستغلاله، يتميز بالقدرة على التأثير على جسمين منفصلين في نفس الوقت ومهما كانت المسافة الموجودة بينهما تمثل فرصة مغرية، حرك الكثير من العقول للبحث عن الطرق الممكنة للاستفادة من التشابك الكمي كمصدر حديث في هذا المجال، حيث نتج عنه عدد من التطبيقات المذهلة بكل حق.

(1−II)جدول يوضح بعض البوابات الكمومية

البوابة	الترميز	المصفوفة
الهاد مار		$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$
باولي −X−		$X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
باولي −Y−		$Y=\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$
باولي −Z−		$Z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$
الطور −s−		$S=\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
$\frac{\pi}{8}$		$T=\begin{bmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{bmatrix}$
بوابة التحكم NOT (controlled− NOT)		$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$
Swap		$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$
بوابة التحكمZ−− (controlled−Z−)		$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{bmatrix}$

بوابة التحكم –S– (controlled–phase)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$
Toffoli		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$
فريكين–Fredkin (controlled–swap)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

القياس		هو الاسقاط الحالة على $\|0\rangle$ و $\|1\rangle$
بت كلاسيكية كوبت		سلك يحمل بت كلاسيكي واحد سلك يحمل كوبت واحد (من اليمين الى اليسار)
n–كوبت		سلك يحمل n–كوب

2.II.من الديناميات الى البوابات الكمومية

الظواهر الفيزيائية المستخدمة لتحقيق التلاعب المطلوب من الكم يمكن ان تكون حالة النظام متنوعة جدا متل ترميز الكوبت في الجزيئات تدور الكم الميكانيكية (سبين) ويتم تنفيذ المنطق عن طريق التلاعب في اتجاه السبين وذلك باختلاف المجال المغناطيسي التطبيقي في اتجاهات مختلفة او إذا تم ترميز الكوبت في حالة الاستثارة الداخلية للأيون يمكن تحقيق عملية البوابة باختلاف الوقت يسمح شعاع الليزر للأشعة الايون او بواسطة مختلف الطول الموجي للضوء الليزري.[5]

لتجسيد بوابة منطقية كمية باسم ميكانيك الكم تخضع لتطور نظام كمومي معزول والتحويل الذي يحققه من خلال معادلة شرو نجر

$$i\hbar\partial \mid \psi\rangle/\partial t = \mathcal{H} \mid \psi\rangle \qquad (1.II)$$

حيت: $\mathcal{H}$ الهاميلتونيان لتحديد الحقول والقوات الفعلية في العمل وهكذا فان المصفوفات الوحدوية التي تصفها تربط بوابات الكم الى العمليات الفيزيائية التي يتم تحقيقها عبر المعادلة :

$$\cup = e^{(\frac{i\mathcal{H}t}{\hbar})} \qquad (2.II)$$

هنا $\mathcal{H}$ الهاميلتونيان يحدد التفاعلات الموجودة في النظام الفيزيائي .

تطور النظم الكمية عندما تكون الحالة $\mid \psi 0\rangle$ في النظام كمومي يتطور في زمن الى الحالة t

$$\mid \psi(t)\rangle = e^{(\frac{i\mathcal{H}t}{\hbar})} \mid \psi(0)\rangle = \cup \mid \psi(0)\rangle \qquad (3.II)$$

حيث $\cup$: تحويل وحدوي.

هذا يعني ان البوابات المنطق الكمومي تعمل على حاسوب كمومي معزول،النظير الكلاسيكي الأقرب الى البوابات المنطقية الكمومية هي البوابات الكلاسيكية القابلة للعكس مثل $NOT - SWAP - FREDKIN$ $TOFFOLI - CNOT$ –[5].

1.2.IIخصائص البوابات الكمومية الناتجة عن الوحدة

الخصائص الأساسية للبوابات المنطقية الكمية تتدفق من تللك الحقيقة يتم وصفها من قبل المصفوفة أحادية ،وهي عبارة عن مصفوفة وحدوية تتحقق اذا وفقط كانت قابلة للعكس أي $U^{-1}=U^*$يساوي تحويل المرافق.[5]

تكونU وحدوية إذا تحقق ما يلي:

U^* وحدوية

U^{-1} وحدوية

$U^{-1}=U^*$ (هو معيار نحديد الوحدة)

$U^*U= 1$

$|\boldsymbol{det}(U)|=\mathbf{1}$هرمتية

$\sum_{i=1}^{2^n}|U_{ij}|^2 = 1$ لعمود تابت

$\sum_{j=1}^{2^n}|U_{ij}|^2 = 1$لصف تابت

$U= \boldsymbol{e}^{(i\mathcal{H})}$،حيت $\boldsymbol{\mathcal{H}}$ تكون مصفوفة هرمتيه$\mathcal{H}^+ = \boldsymbol{\mathcal{H}}$

أي بوابة كمومية قابلة للعكس منطقيا يعني انه إذا بدأت مع حالة كمومية طبيعية بشكل صحيح والعمل عليها سينتهي بك الامر مع حالة الكم الطبيعية وبالتالي ولايوجد احتمال "التسريب"حقيقة ان

$|\boldsymbol{det}(U)|$تكون مقيدة

يعني ان القيدالمحدد يمكن ان يكون: $\pm\boldsymbol{i}$او$\pm\mathbf{1}$ $= |\boldsymbol{det}(U)|$ وبالتالي فان عناصر المصفوفة الموحدة تسمح بشكل معمم بان تكون ارقام معقدة.[5]

2.2.II بوابات ذات بت الكمي واحد

1 .مصفوفات باولي

بالنسبة للكوبت الواحد نعرف مصفوفات باولي ب (X−Y−Z−II) تتميز بالوحدوية والهرمتية هي ذات أهمية خاصة لان أي بت كمومي واحد يكون دائما هاميلتونيان

متال: اذا كان a و b هما مصفوفتان ومصفوفة bهو عكس المصفوفة a فان a*b=1الناتج يكون عبارة عن مصفوفة وحدوية تكتب مصفوفات باولي بالشكل التالي :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad II = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad (4.II)$$

مؤثرات على فضاء 1-كوبت (بت كمي)

$$\{|0\rangle, |1\rangle\} = \left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right\}$$

مثال:

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$X^{+}X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$Z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$Z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$

1.1 .بوابة (Phase): رمزهاS تعرف بالمصفوفة

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad (5.II)$$

2.1 . بوابة $\frac{\pi}{8}$:وهي تعميم للمصفوفة Sرمزها T تعرف بالمصفوفة

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} \qquad (6.II)$$

$$T(\theta) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\,0\rangle$$

$$T(\theta) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = \begin{pmatrix} 1 \\ e^{i\theta} \end{pmatrix} = e^{i\theta}|\,1\rangle$$

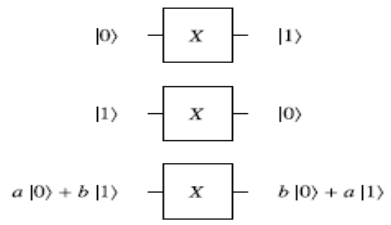
2.بوابة النفي Not

البوابة الكمومية للنفيNOTهي عبارة عن مرادف للبوابة الكلاسيكية xمصفوفة باولي قابلة للعكس

$$\mathrm{X} \equiv \mathrm{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (7.\mathrm{II})$$

تقوم البوابة Not بنفي الحالة الأساسية للحساب $|0\rangle$ او$|1\rangle$ الى $|1\rangle$ و$|0\rangle$ بالترتيب.

$$\begin{cases} NOT\,|\,0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |\,1\rangle \\ NOT\,|\,1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\,0\rangle \\ NOT(a\,|\,0\rangle + b|\,0\rangle) = b\,|\,0\rangle + a|\,1\rangle \end{cases}$$



الصورة (1.II)

3. بوابة $\sqrt{NOT}$

تعد بوابة $\sqrt{NOT}$واحدة من ابسط البوابات الغير الكلاسيكية التي يمكنان نصادفها تكتب

$$\sqrt{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{1/2} = \begin{pmatrix} \frac{1}{2}+\frac{i}{2} & \frac{1}{2}-\frac{i}{2} \\ \frac{1}{2}-\frac{i}{2} & \frac{1}{2}+\frac{i}{2} \end{pmatrix} \qquad (8.II)$$

بوابة $\sqrt{NOT}$لها خاصية التكرار فهي تعادل العملية NOT لكن ينتج عن تطبيق واحد في الحالة الكمومية عدم مع البت الكلاسيكي 0و1بوابة $\sqrt{NOT}$هي اول بوابة غير كلاسيكية صادفناها [5]

$$|0\rangle\sqrt{NOT}\left(\frac{1}{2}+\frac{i}{2}\right)|0\rangle+\left(\frac{1}{2}-\frac{i}{2}\right)|1\rangle\sqrt{NOT}|1\rangle$$

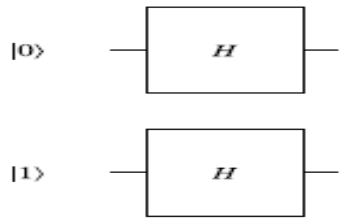
$$|0\rangle\sqrt{NOT}\left(\frac{1}{2}-\frac{i}{2}\right)|0\rangle+\left(\frac{1}{2}+\frac{i}{2}\right)|1\rangle\sqrt{NOT}|0\rangle$$

4 .بوابة الهاد مار"Hadamard"

نرمز لبوابةالهاد ماربH تعد من أكثر البوابات عموما تعمل على بت كمومي واحد البوابة Hيتم تعريفها من خلال المصفوفة

$$\mathrm{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad (9.II)$$

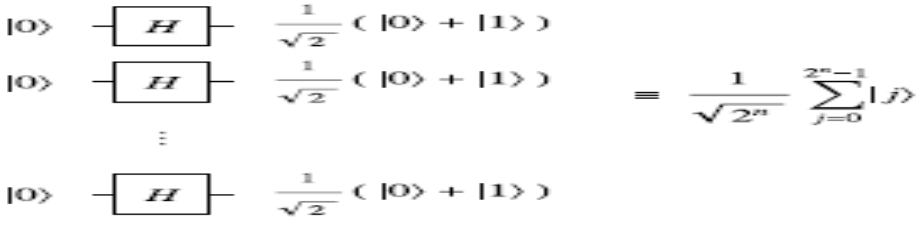
تعمل على تعين الحالات الأساسية للحساب في حالة التراكب الكمومي والعكس صحيح



$$H|1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

$$H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$

الصورة (2.II) توضح تأثير بوابة H على الحالة الأساسية



الصورة (3.II) توضح تأثير البوابة H على عدة بتات كمومية

بتطبيق البوابة H بشكل مستقل على عدة بتات كمومية كلها في نفس الحالة الأساسية أي تم تحضيرها في الحالة $|0\rangle$ إيمكننا انشاء تراكب عدة بتات كمومية تكون الحالة الناتجة عبارة عن تمثيل ثنائي

اذا تم تحضير بت كمومي في حالة $|0\rangle$ ونطبقH على كل بت كمومي تكون الحالة الناتجة في تراكب متساو لجميع الاعداد في النطاق من 0 الى2^n.

$$H|0\rangle \otimes H|0\rangle \otimes H|0\rangle \otimes H|0\rangle \dots\dots\dots\dots\dots \otimes H|0\rangle \qquad (10.II)$$

يمكننا انشاء تراكب من عدة بتات كمومية مكونة من2^n تمثل سجلات كل سلاسل البت الممكنة التي يمكن كتابتها باستخدام n–بت كمي.

أهمية البوابة H انها تعطي القدرة على تحميل اضعاف العديد من المؤشرات الى كمبيوتر كمومي باستخدام العديد من العمليات متعددة الحدود فان الحوسبة الكمومية يمكن ان تكون اقل إمكانية لتحقيق اختراقات في تعقيد الحساب.[5]

البرهان:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0.1\}^n} (-1)^{xy}|y\rangle$$

$$H|a\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a|1\rangle) \qquad ; a = 0.1$$

$$H|a\rangle = \frac{1}{\sqrt{2}} \sum_{b\in\{0.1\}^n} |b\rangle(-1)^{ab}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\{|0\rangle(-1)^0 + |1\rangle(-1)^{0.1}\} = \frac{1}{\sqrt{2}}\{|0\rangle + |1\rangle\}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\{|0\rangle(-1)^{1.0} + |1\rangle(-1)^{1.1}\}$$

في حالة 2-بت كمومي

$$|x\rangle = |x_1x_2\rangle = |x_1\rangle|x_2\rangle$$

$$H^{\otimes 2}|x_1\rangle = H|x_1\rangle H|x_2\rangle$$

$$= \frac{1}{\sqrt{2}}\sum_{y_1\in\{0.1\}}|y_1\rangle(-1)^{x_1y_1}\frac{1}{\sqrt{2}}\sum_{y_2\in\{0.1\}}|y_2\rangle(-1)^{x_2y_2}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y_1 \in \{0.1\} y_2 \in \{0.1\}} (-1)^{x_1 y_1 + x_2 y_2} \mid y_1 y_2 \rangle$$

$$= \frac{1}{\sqrt{2^2}} \sum_{y \in \{0.1\}^2} (-1)^{xy} \mid y \rangle$$

-في حالة عدة بتات كمومية

$$H^{\otimes n} \mid x \rangle = H \mid x_1 \rangle H \mid x_2 \rangle \dots \dots \dots \dots \dots \dots H \mid x_n \rangle$$

$$= \sum_{y_1 \in \{0.1\}} \sum_{y_1 \in \{0.1\}} (-1)^{x_1 y_1} \sum_{y_2 \in \{0.1\}} (-1)^{x_2 y_2} \dots \dots . \sum_{y_n \in \{0.1\}} (-1)^{x_n y_n}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y \in \{0.1\}^n} (-1)^{xy} \mid y \rangle \qquad ; \mid y \rangle \mid y_1 y_2 \dots \dots \dots . y_n \rangle$$

5.الدوان حول المحاور X-Y-Z

بعد ان تعرفنا على بعض البوابات المنطقية الكمية مثل $-\sqrt{NOT}$ Hadamard-NOT ننتقل الى نوع اخر ويعد اكتر شيوعا من البوابات السابقة .

البوابات ذات البت الكمومي الواحد، ولمعالجة هذه المسألة يجب علينا أولا تقديم عائلة البوابات الكمية التي تؤدي التناوب حول ثلاث محاور متعامدة بشكل متبادل في فضاء بلوخ (كرة بلوخ) يتم في هذا الفضاء بتمثيل البت الكمومي النقي بنقطة على سطح كرة بلوخ وذلك بتأثير بوابة ذات بت كمومي واحد التي تعمل على تعين النقط الأخرى على سطح كرة بلوخ.

البوابة التي تقوم بتدوير الحالة $\langle 0 \mid$ و$\langle 1 \mid$ حول المحاور الثلاثx.y.zتعتبر هذه المحاور ذات أهمية خاصة لأنها تمكننا من تحليل التعسفي لبوابة الكم المفردة البت الكمومي في تسلسل من البوابات الدورية

يتم تعريف الحالة النقية باختيار ثلاث محاور متعامدة بشكل متبادلx.y.zأوما يعادل ذلك ثلاث احداثيات قطبيةنصف القطرR(وهو وحدة لجميع النقاط على سطح كرة بلوخ)

الزاويةθ تمثل خط العرض تقاس من القطب الشمالي الى القطب الجنوبي محصورة في

مجال $(0 \leq \theta \leq \pi)$

الزاوية $\boldsymbol{\phi}$(تمثل خط الطول تدور حول المحور Z في اتجاه عقارب الساعة) بحيث يمكن تحديد أي نقطة على سطح كرة بلوخ باستخدام احداثيات (X.Y.Z) او ما يكافئهامن إحداثيات ($\theta.R.\boldsymbol{\phi}$)

لا تعطينا النتيجة مضبوطة لذلك يجب تحديد عامل طور بصورة شاملة هذين النظامين مرتبطان عبر معادلة [5]

$$X = \sin(\theta)\cos(\theta) \qquad (11.II)$$

$$Y = \sin(\theta)\sin(\phi) \qquad (12.II)$$

$$Z = r\cos(\theta) \qquad (13.II)$$

البوابات الكمية التي تدور حول المحاور X−Y−Zموضحة في الاشكال (4.II)و(5.II)و(6.II) يمكن بناءها من استخدام مصفوفات باولي X−Y−Zوالمصفوفة الحيادية $\boldsymbol{I}$ لتحقيق التحويل العالمي الشامل نحدد المصفوفات التالية :

$$R_X(a) = e^{(-ia\frac{X}{2})} = \begin{bmatrix} \cos(\frac{a}{2}) & -i\sin(\frac{a}{2}) \\ -i\sin(\frac{a}{2}) & \cos(\frac{a}{2}) \end{bmatrix} \qquad (14.II)$$

$$R_y(a) = e^{\left(-ia\frac{y}{2}\right)} = \begin{bmatrix} \cos\left(\frac{a}{2}\right) & -\sin\left(\frac{a}{2}\right) \\ \sin\left(\frac{a}{2}\right) & \cos\left(\frac{a}{2}\right) \end{bmatrix} \qquad (15.II)$$

$$R_Z(a) = e^{(-ia\frac{Z}{2})} = \begin{bmatrix} e^{-i\frac{a}{2}} & 0 \\ 0 & e^{i\frac{a}{2}} \end{bmatrix} \qquad (16.II)$$

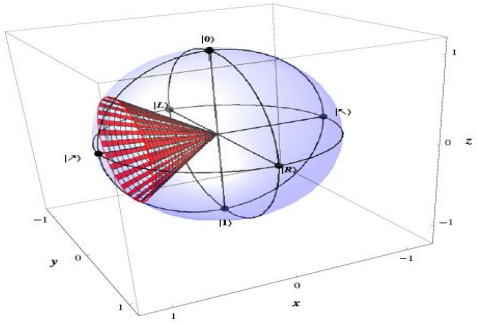
$$Ph(\delta) = e^{(i\delta)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad (17.II)$$

مثال: نطبق البوابة$R_X(a)$ على الحالة $|\psi\rangle$

$$R_X(a)\,|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{(i\phi)}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

الصورة (4.II) تقوم البوابة$R_X(a)$ بتعين الحالة$|\psi\rangle$ على سطح كرة بلوخ الى الحالة جديدة

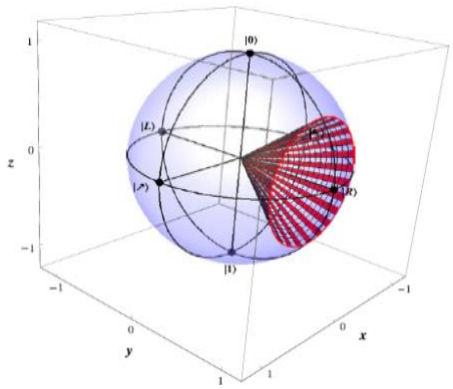
$$R_X(a)\,|\,\psi\rangle = \cos\left(\frac{\theta}{2}\right)|\,0\rangle + e^{(i\phi)}\sin\left(\frac{\theta}{2}\right)|\,1\rangle$$



لصورة (4.II)

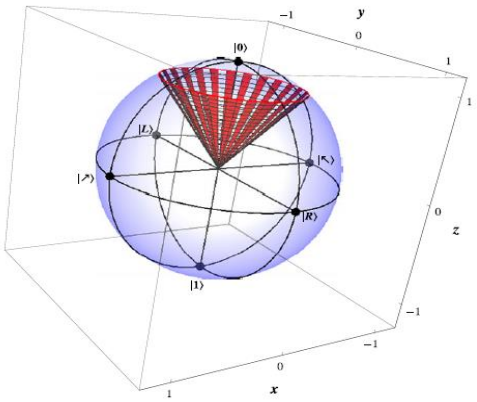
ممثلة بنقطة تم الحصول عليها بتدويرمتجه من مركز R كرة بلوخ للحالة$|\psi\rangle$ بزاوية تقدر ب$\frac{\theta}{2}$حول المحور Xللعودة الى الحالة الاصلية نقوم بتدويرب4π.[5]

الصورة (5.II) توضح البوابة $R_Y(a)$ بتعين الحالة $|\psi\rangle$ على سطح كرة بلوخ الى الحالة جديدة$R_Y(a)\,|\,\psi\rangle$ ممثلة بنقطة تم الحصول عليها بتدويرمتجه من مركز R كرة بلوخ للحالة$|\psi\rangle$ بزاوية تقدر ب$\frac{\theta}{2}$ حول المحور y للعودة الى الحالة الاصلية نقوم بتدوير4π.[5]



الصورة (5.II)

الصورة (6.II) توضح البوابة $R_Z(a)$ بتعين الحالة$|\psi\rangle$ على سطح كرة بلوخ الى الحالة جديدة$R_Z(a)\,|\,\psi\rangle$ ممثلة بنقطة تم الحصول عليها بتدويرمتجه من مركز R كرة بلوخ للحالة$|\psi\rangle$ بزاوية تقدر ب$\frac{\theta}{2}$ حول المحور z للعودة الى الحالة الاصلية نقوم بتدويرب4π.[5]



الصورة (6.II)

التناوب على مجال بلوخ لا يتطابق مع الحدس المنطقي الذي تعلمناه من تجربة العالم اليومي عادة يكون التناوب 2π راديان أي (360 درجة) لكائن صلب حول أي محور يعيده الى اتجاهه الأول

من اجل العودة الى الحالة الأولية في مجال بلوخ يجب علينا تدوير الحالة الكم بزاوية تقدر ب4π.[5]

6. انتاج بوابة$\sqrt{NOT}$−Hadamard− NOT من بوابات التناوب

يمكن الحصول على بوابة$\sqrt{NOT}$−Hadamard− NOTعن طريق بوابات التناوب كما هو موضح في المعادلات التالية:

$$\mathrm{NOT} \equiv R_x(\pi).Ph(\pi) \qquad (18.II)$$

$$\mathrm{NOT} \equiv R_y(\pi)R_z(\pi).Ph\left(\frac{\pi}{2}\right) \qquad (19.II)$$

$$\sqrt{\boldsymbol{NOT}} \equiv R_x\left(\frac{\pi}{2}\right).Ph\left(\frac{\pi}{4}\right) \qquad (20.II)$$

$$\sqrt{\boldsymbol{NOT}} \equiv R_z\left(-\frac{\pi}{2}\right).R_y\left(\frac{\pi}{2}\right).R_z\left(\frac{\pi}{2}\right).Ph\left(\frac{\pi}{4}\right) \qquad (21.II)$$

$$H \equiv R_x(\pi).R_y\left(\frac{\pi}{2}\right).Ph\left(\frac{\pi}{2}\right) \qquad (22.II)$$

$$\mathrm{H} \equiv R_X\left(\frac{\pi}{2}\right).R_z(\pi).Ph\left(\frac{\pi}{2}\right) \qquad (23.II)$$

7 .تحلل البوابةR_x

خشيه ان يبدو غريبا ان نتمكن من تحقيق التعسفي−لبوابة1−كوبت بدون أداء دوران حول محور x نلاحظ انه من الممكن التعبيرعن التناوب حول المحور السيني فقط من حيث الدوران حول محورy و z.

$$R_X(\theta) = e^{(-i\theta\frac{X}{2})} = \begin{bmatrix} \cos(\frac{\theta}{2}) & i\sin(\frac{\theta}{2}) \\ i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{bmatrix} \qquad (24.II)$$

$$\equiv R_z\left(-\frac{\pi}{2}\right).R_y(\theta).R_z\left(\frac{\pi}{2}\right)$$

$$\equiv R_y\left(\frac{\pi}{2}\right).R_z(\theta).R_y\left(-\frac{\pi}{2}\right)$$

3.2.II بوابة الكم الخاضعة للرقابة(Controlled Quantum Gates)

لإجراء عمليات حسابية من الضروري تغير العملية نطبقها على مجموعة واحدة من الكوبت اعتمادا على مجموعة أخرى من الكوبت وتسمى البوابات التي تنفذ هذه العملية هي إذا" "ثم" "نوعاما" هذا النوع من البوابات يتم التحكم فيه. بعض الأمثلة على البوابات الخاضعة للرقابة هي بوابة C–Not (يتم التحكم في البوابة النفي Controlled-NOT) وفريكينFREDKIN(يتم التحكم في بوابة SWAP) وبوابة TOFFOLI(يتم التحكم في تحكم بوابة النفي Controlled–Controlled–NOT).

تأثر على الأساس الحسابي على سيبل المثال تحول CNOTالقاعدة الحسابية تنص على ان الجزء الثاني يكون منفي إذا وفقط كان الكوبت الأول في الحالة ⟨1 | .[5].

$$\begin{aligned} |00\rangle CNOT\ |00\rangle \\ |01\rangle CNOT\ |01\rangle \\ |10\rangle CNOT\ |11\rangle \\ |11\rangle CNOT\ |10\rangle \end{aligned} \qquad (25.\text{II})$$

وبالتالي يتم التحكم في قيمة كوبت الثاني يطلق على كوبت الأول التحكم "CONTROL "

$$CNOT\ (a|0\rangle + b|1\rangle)|0\rangle = |00\rangle + |11\rangle$$

بالمقابل تعمل البوابةفريكين" FREDKIN "على النحو التالي الكوبت الثاني والثالث يكون مبادلة اذا وفقط كان كوبت الأول في الحالة ⟨1 |البوابة فريكين تنفذ عملية مبادلة «swap» متحكم بها.

$$|011\rangle \text{FREDKIN} |011\rangle$$

$$|100\rangle \text{FREDKIN}\ \ |100\rangle$$

$$|101\rangle \text{FREDKIN}\ \ |110\rangle$$

$$|110\rangle \text{FREDKIN} |101\rangle$$

$$|111\rangle \text{FREDKIN}\ \ |111\rangle$$

عمل بوابة TOFFOLIهو نفي كويت الثالث (كوبت الهدف) اذا وفقط كوبت الأول و الثاني يكون في الحالة $|11\rangle$ فان بوابةTOFFOLIلديها كوبتين من التحكم في كوبت هدف

$|000\rangle$ TOFFOLI $|000\rangle$

$|001\rangle$ TOFFOLI $|001\rangle$

$|010\rangle$ TOFFOLI $|010\rangle$

$|011\rangle$ TOFFOLI $|011\rangle$

$|100\rangle$ TOFFOLI $|100\rangle$

$|101\rangle$ TOFFOLI $|101\rangle$

$|110\rangle$ TOFFOLI $|111\rangle$

$|111\rangle$ TOFFOLI $|110\rangle$

البوابات C–NOT –TOFFOLI – FREDKIN هي بوابات كلاسيكية قابلة للعكس بالإضافة انها بوابة كمومية بسبب التحويلات التي تؤديها .

التبديل الحسابي للحالة الأساسية لذلك يجب ان تكون وحدوية لكن في الواقع يمكن للبوابة الكمية الخاضعة للرقابة تكون اكثر تطورا من البوابة الكلاسيكية المحكومة، طبيعة التعميم الكمي للبوابة الخاضعة للرقابة CNOTهو البوابة U المتحكم فيها.

بحيث$\begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$ هو بوابة 1-كوبت التعسفي. $Controlled - U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{bmatrix}$

4.2.II البوابة O_f "*Oracles*"

البوابة O_fهي تعميم C-NOT تعمل على n–qbit نرمز لها بالرمز O_f فكرة **"*Oracles*"**

هو عبارة عن صندوق اسود يقوم بإدخال عدد من كوبت (n−qbit) وإخراج دالة f(x) كما قابل للانعكاس تماما مثل أي دائرة كلاسيكية أخرى ندخل Xو Yيخرج X⊕Y

"*Oracles*" في حالة الكم هو صندوق الأسود الذي يأخذ n−كوبت ويقوم بالتحويل الوحدوي U عليهم بحيث يمكن ادخال 2−كوبت سجلات الكم وتحويلها وفق مايلي :

$$|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle \qquad (26.II)$$

في ميكانيك الكم هناك احتمالات أخرى بحيث يمكننا التحويل

$$|x\rangle = (-1)^{f(x)}|x\rangle \qquad (27.II)$$

ينفذ إزاحة الطور استنادا الى قيمةf(x) الحسابات التي تنطوي على **"*Oracles*"** ترتكز عادة على تحديد جزء من خاصية الدالة f(x) يتم تحديد f(x) بواسطة الصندوق الأسود يكون مهم إذا كانت الدالة f(x)معروفة فهذه الخاصية غير مضمونة بما فيه الكفاية ان معرفة f(x)تحدث اختلافا في الحالات كما ان الفرق ليس واضح بين مشكلة الاوراكل والحساب العادي [6].

في العموم من اجل n−qbit نعرف O_f

نعرف o_f بF دالة كثيفة

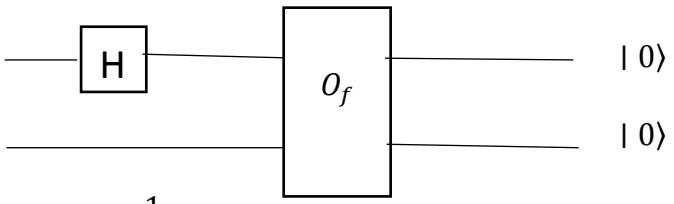
$$F: \{0,1\}^n \rightarrow \{0,1\}^m \qquad (28.II)$$

$$|a\rangle|b\rangle O_f \rightarrow |a\rangle|b \oplus f(a)\rangle$$

$$|a\rangle|b\rangle \rightarrow O_f \rightarrow |a\rangle|b \oplus a\rangle$$

مثال:$\frac{1}{\sqrt{2}}\{|0\rangle + |1\rangle\}\otimes|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

(7-II) رسم تخطيطي لبوابة O_f



$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|01\rangle+|11\rangle) \rightarrow \frac{1}{\sqrt{2}}(|01\rangle+|11\rangle)$$

3.IIالتشابك الكمي

التشابك الكمي هو ظاهرة كمية ترتبط فيها الجسيمات الكمية (الفتونات، الالكترونات ، الجزيئات) ببعضها رغم وجود مسافة كبيرة تفصل بينها مما يقود الى ارتباطات في الخواص الفيزيائية المقاسة لهذه الجسيمات الكمية.ان المقصود بالتشابك الكمومي هو حالة الترابط التي تنشأ بين مجموعة من الأنظمة التي تفاعلت مع بعضها البعض فتشابكت الحالات الكمية لهذه الأنظمة بحيث صارة من غير الممكن وصف أحدها بمنأى عن الاخر، أي لا نظير كلاسيكي له فلا يوجد أي مفهوم في الفيزياء الكلاسيكية يضاهي التشابك الموجود في ميكانيك الكم وقد استخدمه في مفارقة EPR.لشرح التشابك سنقوم بدراسة انشاء وتدمير زوج من EPR يدعى من قبل آينشتاينEnstine، بودولسكيPodolsky،روزينRosen

لكن ما هو جسيم EPR؟ إنها جسيمات تأتي دائمًا زوجًا زوجًا. وهي تعبِّر بامتياز عن ظاهرة كوانتية بحتة معروفة باسم "التشبيك intrication" (entanglement). وهي، باختصار، ظاهرة لا مكافئ لها في الفيزياء الكلاسيكية. كان الفيزيائي دافيد بوم قد عرضها وفق الصيغة المبسطة التالية: يمكن لفوتونين ضمن ظروف معينة أن يصدرا من المنبع نفسه بحيث أن استقطابهما يكون متعاكسًا مهما كان القياس الذي يخضعان له طالما كان القياس نفسه. يشكل هذان الفوتونان عندها زوجًا من الجسيمات EPR. فإذا قسنا استقطاب أي من الفوتونين عند أي زاوية كانت فإننا سنعرف عندها كيف سيتفاعل الفوتون الثاني عند

تطبيق القياس نفسه عليه. وليس للموضعين النسبيين للفوتونين في لحظة القياس أية أهمية. فيمكن أن يكونا عند طرفي المجرة المتقابلين، ويؤكد لنا الميكانيك الكمومي أن ذلك لن يغير من النتيجة!

كان ألبرت أينشتاين قد برهن في عام 1935 بالتعاون مع بوريس بودولسكي وناثان روزن، أن التشابك intrication كان نتيجة محتمة لقوانين الميكانيك الكمومي. ولا بد أن نعرف أن أينشتاين، قد أمضى جزءًا طويلاً من حياته وهو يسعى للبرهان أن هذه النظرية غير كاملة على هذا النحو. ولنكن دقيقين، فهو لم يكن يشكك بتنبؤاته النظرية، بل على العكس كان يعتقد بوجود حقيقة تحتية كانت تسمح بتفسير هذه النتائج والأفكار. وكان يرى بشكل خاص أن جهازًا للقياس لا يستطيع سوى الكشف عن المعلومات الموجودة سلفًا في المنظومة المقاسة: وهذا ما كان يسميه "عناصر الحقيقة". وعلى العكس تمامًا، كان الميكانيك الكمومي وعلى رأسه نيلز بور يؤكد أن هذه "الحقيقة" ليست سوى "خديعة": فهي غير موجودة قبل أن يجبرها جهاز القياس على الظهور. على سبيل المثال، إذا قيس فوتون مستقطب عموديًا بشكل قطري، فليس ثمة ما يجبره على الاختيار بين أكثر من 45 درجة أو أقل من 45 درجة، حيث للنتيجتين الحظ نفسه بالتحقق والظهور. ووفقًا للميكانيك الكمومي، لا يمكن لأي فوتون أن يحصل إن صح التعبير على استقطاباته الخطية (الأفقية مقابل العمودية) والقطرية (أقل أو أكثر من 45 درجة) المحددة بشكل آني متزامن. للوهلة الأولى، يبدو أن التشبيك يثبت وجود عناصر الحقيقة هذه التي تحدث عنها أينشتين. وكانت حجة أينشتين، التي عدَّلها بوم، هي أن استقطاب الفوتون غير المقاس بواسطة زوج من الـ EPR يجب أن يتوافق مع عنصر من عناصر الحقيقة هذه. ويتحدد هذا الأخير أيًا كانت زاوية قياس الاستقطاب طالما أن هذه المعلومة يمكن أن تعرَّف دون أن يكون عليها التفاعل مع الفوتون. وحده الفوتون الآخر في زوج الفوتونات هذا يتخلخل بواسطة جهاز القياس.

فاذا امكن كتابة الحالة الكلية للنظام على شكل جداء تنسوري لحالة كل نظام جزئي على حدى، فان النظامين غير متشابكين وحالة كل منهما هي حالة نقية وحالة النظام قابلة للفصل أو غير متشابكة. في الحالة العكسية أين يكون من غير الممكن فصل حالة النظام الكلي الى حالتي قسميه فان هذه الحالة تدعى بالحالة المتشابكة فعلى سبيل المثال يمكن أن نجعل جسمين في حالة كمية متشابكة مثلspin السبين فاذا قسنا دوران أحدهما وتبين أنه ذو دوران علوي (↑) فالأخر حتما يكون ذو دوران سفلي (↓) يجب أن نتذكر هنا ان نتيجة القياس للجسم الكمومي عشوائية تماما حسب تفسير" كوبنهاغن " المعتمد ولا يمكنا التنبؤ بنتائج هذا القياس ومع ذلك فان عملية القياس المجراة على جملة كمومية تأثر انيا على جمل كمومية أخرى متشابكة مع الأولى رغم أن سرعة نقل المعلومة تخترق مبدأ سرعة الضوء العظمى في النسبية فانه لايمكن نقل معلومات كلاسيكية عن طريق التشابك الكمي مما يسمح بالحفاظ على النسبية.[7.8.9]

H تم نطبق عليها الهادمافي الحالة$|0\rangle$ انفترض أول كوبت $|\psi\rangle$

$$|\psi_1'\rangle = H\,|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad (29.II)$$

الان نأخذ كوبت اخر $|\psi_2\rangle$ في الحالة صفر$|0\rangle$

$$|\psi_1'\rangle \otimes |\psi_2\rangle = |\psi_1'\psi_2\rangle = \frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + 0|11\rangle \qquad (30.II)$$

الان نطبق بوابة C–NOT

$$|(\psi_1'\psi_2)''\rangle = \mathrm{CNOT}\,|\psi_1'\psi_2\rangle$$

$$= \begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{bmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

مفتاح التشابك هو الخاصية التي لا يمكن ان تتجزأ أي انه لا توجد حالة كم في حالتين الأولى والثانية

في نفس الزمن الجداء التو نسوري السابق يوضح ذلك $|\psi_1'\rangle \otimes |\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

لتوضيح سبب التشابك نقوم بإجراء القياس قبل تطبيق بوابة C–NOT

$$M_{1_2} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ و} \qquad M_{0_2} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

قبل القياس كان النظام في الحالة

$$|\psi_1'\rangle \otimes |\psi_2\rangle = |\psi_1'\psi_2\rangle = \frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + 0|11\rangle \qquad (29.\text{II})$$

من الواضح أن قياس كوبت الثاني سيكون في الحالة$|0\rangle$ لاحظ أن $M_{02}' M_{02} = M_{02}$وبالتالي

$$\mathrm{P}(0) = \langle\psi_1'\psi_2| \, M_{02}'M_{02}|\psi_1'\psi_2\rangle = \langle\psi_1'\psi_2| \, M_{02}|\psi_1'\psi_2\rangle \qquad (31.II)$$

$$= \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = 1$$

بعد القياس نتحصل على:

$$\frac{\mathrm{M_m}|\psi\rangle}{\sqrt{\langle\psi|\mathrm{M^\dagger{}_m M_m}|\psi\rangle}} = \frac{\begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}}{1} = |\psi'_1\psi_2\rangle$$

يمكننا أن نرى أن القياس لم يكن له تأثير على الكوبت الأولى يبقى في تراكب بين 0 و 1

نقوم بالقياس لكن بعد تطبيق البوابة C-NOT:

$$|\psi\rangle = |\psi_1'\psi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

ليس من الواضح أن كانت كوبت الثانية ستعود الى الحالة 0أو 1 أو تكون في كلا الحالتين بالتساوي

ولرؤية هذا يمكننا حساب الاحتمال للحصول على الحالة$|0\rangle$

$$P(0) = \langle\psi | M_{02}'M_{02}|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad (32.II)$$

$$= \begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}}\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\0\\0\end{bmatrix} = \frac{1}{2}$$

لدينا نصف فرصة للحصول على الحالة $|0\rangle$ بعد القياس

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M^{\dagger}{}_m M_m|\psi\rangle}} = \frac{1}{\sqrt{\frac{1}{2}}}\begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{bmatrix} = \frac{1}{\sqrt{\frac{1}{2}}}\begin{bmatrix}\frac{1}{\sqrt{2}}\\0\\0\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} = |00\rangle$$

هذا هو الشيء المميز حول التشابك الكمومي من خلال قياس كوبت واحد يمكن أن تؤثر على احتمال السعات من الكوبت الأخرى في النظام يعد التشابك تحدي مفتوح في الحوسبة الكمومية حيث تكمن الصعوبة عدم وجود أي تناظر كلاسيكي، التشابك يربط البتات الكمومية لكن لا يخلق المزيد منها.[1]

II .4.تطبيقات التشابك الكمي

II-4-1نظرية عدم الاستنساخ *(No-CloningTheorem)*

البوابات الكمية هي النسخة عن البوابات المنطقية الكلاسيكية التي تستخدم في الدارات الإلكترونية للحواسيب والأجهزة الإلكترونية. تتعدد البوابات المنطقية وتختلف. باختلاف العملية التي تؤديها، أحد هذه البوابات المنطقية هي بوابةXOR وهي النظير الكلاسيكية لبوابةC-NOT، بوابةCNOTلا تقدم نسخ البت الكمي والسبب في ذلك هو إمكانية تراكب الحالات الكمية نتيجة لخطية ميكانيك الكم، فرغم أن هذه البوابة قادرة على نسخ الحالتين الكميتين $(|0\rangle\ |1\rangle)$ بشكل مماثل للحالة الكلاسيكية

$$\begin{cases} |\ 00\rangle CNOT|\ 00\rangle \\ |\ 10\rangle CNOT|\ 11\rangle \end{cases} \quad (25.II)$$

إلا أنها لا تستطع من جهة أخرى أن تنسخ أي تركيبة خطية من الحالتينالسابقتين من بِت التحكم إلى بِت الهدف.

$$\text{CNOT}\ (a|0\rangle + b|1\rangle)|0\rangle = |00\rangle + |11\rangle$$

هذه النتيجة مختلفة عن النتيجة التي ستعطيها آلة نسخ كمية حقيقية :$(a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)$

عجز بوابة CNOT عن نسخ الحالة الكمية قد لا يعني أنه لا يوجد هناك بوابة معينة أو أداة تستخدم تحويلا محددا يملك القدرة على نسخ حالة كمية غر معروفة، لكن قبل الذهاب بعيدا في هذه النقطة قد يكون من المفيد فهم ما الذي قد يعنيه أن يكون من الممكن نسخ أي حالة كمية مجهولة ، فالقدرة على صنع نسخ من حالة كميةغير معروفة يسمح بالتعر ف على هذه الحالة عن طريق تنفيذ عمليات قياس متكررة ومختلفة للتعرف على الحالة الكمية بالدقة المرغوبة كمي فمثلا التعرف على حالة بت كمي – كما سبق وتعرضنا له في الفصل الأول (I–7)

تخيل ان احدهم قد ارسل(Alice) بت كمي الى شخص أخر، المستقبل(Bob) يستطيع صنع عدة نسخ من البت الكمي الذي وصله ومن ثم يقس نسخة وفق ثلاث محاور متعامدة ليتمكن من التعرف على حالة البت الكمي الذي بحوزته الميزة التي يمكن الاستفادة منها هنا هو أن البت الكمي بدل أن ينفل معلومة واحدة كمثيله الكلاسيكي اصبح بإمكانه نقل مجموعة أكبر من المعلومات.

فائدة التعرف على حالة البت الكمي المجهولة بفضل عملية النسخ لا يتوقف هنا بل ان الأمر الأكثر اثارة بشأنها هو القدرة على نقل المعلومات بسرعة أكبر من سرعة الضوء فعليا !! لتصوير كيفية حدوث هذا الأمر نتخيل أنه تم تحضير كوبتات في نفس الحالة حالات الأساس تعرف كما يلي :

$$|\phi\rangle^{+} = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) \qquad |\phi\rangle^{-} = \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$$
$$|\psi\rangle^{+} = \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle) \qquad |\psi\rangle^{-} = \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle) \qquad (33.\text{II})$$

نقوم بإرسال واحدة من ثنائية البت الكمي المتشابك الى المستقبل الذييوجد في مكان بعيد عنoz أوالمرسل. لدى المستقبل القدرة على قياس سبين البت الكمي الذي لديه وفق المحورOx أو وفق المحورOz.

لكن المرسل لا يستطيع أن يميز بواسطة عملية قياس واحدة ان كانت الحالة التي يقيسها هي حالة ذاتيه لS_xأم S_z ولا يستطيع تكرار عملية القياس للتعرف على حالة البت الكمي لأن عملية القياس الأولى قد غيرت حالته، حالته ولهذا استنتجنا سابقا أن ارسال رسالة بسرعة أكبر من سرعة الضوء هو أمر مستحيل لكن لو كانت هناك الة نسخ للبت الكمي فان المرسل يستطيع صنع عدة نسخ من البت الكمي الذي لديه ومن ثم يمكنه تحديد حالته بذات الطريقة التي شرحت سابقا،اذا يمكنه معرفة المؤثر الذي قاسه المستقبل وبالتالي يستطيع قراءة رسالته، مايعني أن هذه الرسالة قد انتقلت بسرعة اكبر من الضوء لقد خرق وجود الة نسخ كمية للتو أحد قوانين النسبية الخاصة ! وهوما يرجع سلفا بأن وجودها هو أمر غير ممكن للتحقق

من هذا نبدأ بوضع الإطار النظري لالة النسخ الكمية لهذه الالة القدرة على نسخ الحالة الكمية لأي بت كمي A الى بت كمي اخر B.

الحالة في موجود $|0\rangle_B$ داخل الالة، تقوم الالة بتطبيق تحويل واحدي معين على كلا البت الكميين ومن ثم تخرجهما في نفس الحالة الكمية, فمثلا ان كان البت الكمي A في الحالة $|\varphi\rangle_A$ فان الالة ستعمل كالتالي :

$$|\varphi\rangle_A\,|0\rangle_B \rightarrow |\varphi\rangle_A\,|\varphi\rangle_B \qquad (34.II)$$

وان كان $|\psi\rangle_A$ فان الة النسخ ستقوم بالعملية الاتية:

$$|\psi\rangle_A\,|0\rangle_B \rightarrow |\psi\rangle_A\,|\psi\rangle_B \qquad (35.II)$$

وعليه فان عمل الة النسخ على الحالة $a|\varphi\rangle_A + b|\psi\rangle_A$ يعطي الحالة:

$$a|\varphi\rangle_A + b|\psi\rangle_B)\,|0\rangle_B \rightarrow a|\varphi\rangle_A|\varphi\rangle_B + b|\psi\rangle_A\,|\psi\rangle_B \qquad (36.II)$$

الة النسخ لم تقم هنا بنسخ حالة البت الكمي A الى البت الكمي B فالحالة التي تم الحصول عليها مختلفة عن الحالة . $(a|\varphi\rangle_A + b|\psi\rangle_A)(a|\varphi\rangle_B + b|\psi\rangle_B)$ التي كنا نرجو الحصول عليها من الة النسخ اذا فقد فشلت الة النسخ في استنتاج الحالة الكمية. بسبب خطية ميكانيك الكم مرة أخرى ولم يكن أداؤها أفضل من أداء بوابة CNOT

ماذا لو حاولنا الان التعميم العملية قليلا بحيث نفرض ان التحويل الذي يعمل على حالتي البت الكميتين ليس واحديا، لكن يمكن أن يمدد ليكون واحديا على فضاء أوسع من فضاء البت الكميتين وعليه نوسع الفضاء الذي تؤثر عليهالة النسخ بالشكل الذي يسمح للتحويل الذي تطبقه أن يكون واحديا وبالتالي فان تأثير الة النسخ على حالتين عشوائيتين $|\varphi\rangle_A|\psi\rangle_B$ من فضاء البت الكمي A هو:

$$\begin{aligned} |\varphi\rangle_A\,|0\rangle_B|\Omega_0\rangle &\rightarrow \quad |\varphi\rangle_A\,|\varphi\rangle_B|\Omega_\varphi\rangle \\ |\psi\rangle_A\,|0\rangle_B|\Omega_0\rangle &\rightarrow \quad |\psi\rangle_A\,|\psi\rangle_B|\Omega_\psi\rangle \end{aligned} \qquad (37.II)$$

أين **Ω** هو المحيط الذي يتأثر بالعملية الواحدية التي تقوم بها الة النسخ (وقد يكون هذا المحيط هو الة النسخ)،$|\Omega_0\rangle$ هي حالة المحيط قبل بدء عملية الاستنساخ ويمكن اعتبارها الحالة الواحدية للمحيط قبل أن تؤثر عليه الة النسخ ، أما $|\Omega_\psi\rangle$و$|\Omega_\varphi\rangle$ فهي حالة المحيط بعد عملية النسخ وقد تعتمد على حالة البت الكمي A وقد لا تعتمد عليها العملية التي تنفذها الة النسخ واحديه ما يعني أن الجداء الداخلي محفوظ وبالتالي :

$$_A\langle\varphi|\psi\rangle_A\ {}_B\langle 0|0\rangle_B\langle\Omega_0|\Omega_0\rangle = {}_A\langle\varphi|\psi\rangle_A\ {}_B\langle\varphi|\psi\rangle_B\langle\Omega_\varphi|\Omega_\psi\rangle \quad (38.II)$$

وعليه فان

$$\langle\varphi|\psi\rangle| = \langle\varphi|\psi\rangle\langle\varphi|\psi\rangle\langle\Omega_\varphi|\Omega_\psi\rangle \quad (39.II)$$

لو أردنا حل المعادلة السابقة من اجل معرفة قيمة الجداء الداخلي $\langle\varphi|\psi\rangle$ فان الأمر سيكون مماثلا لحل معادلة من الدرجة الثانية،الحل الأول لهذه المعادلة هو0=$\langle\varphi|\psi\rangle$أي أن الشعاعين $|\varphi\rangle$ و $|\psi\rangle$ متعامدان وأما الحل الثاني فهو $\langle\varphi|\psi\rangle = \langle\Omega_\varphi|\Omega_\psi\rangle^{-1}$، لكن الأشعة في فضاء هيلبرت الموسع منظمة ما يعني أن أقصى قيمة للجداء الداخلي لهذه الأشعة لاتتعدى الواحد (بقيمة مطلقة)، وعليه لايمكن أن يكون الحل الأخير مقبولا الا اذا كان$|\langle\varphi|\psi\rangle| = \left|\langle\Omega_\varphi|\Omega_\psi\rangle^{-1}\right| = 1$

مايعني أن الشعاع $|\varphi\rangle$ هو نفسه الشعاع $|\psi\rangle$ (قد يختلفان في فرق الطور فقط)وكذلك $|\Omega_\varphi\rangle = |\Omega_\psi\rangle$. باختصار، لاتستطيع آلة النسخ المعممة سوى استنتاج حالات متعامدة فقط وليست قادرة على استنتاج أشعة غير متعامدة، وكل مجموعة متعامدة ومنظمة من الأشعة تنسخها آلة مصممة لتنسخ فقط أشعة تلك المجموعة أو الأساس ما يستلزم معرفة جزئية بحالة البت الكمي المراد استنتاجه.

كل المناقشة السابقة ماهي الا اثبات لنظرية مهمة في ميكانيك الكم تمثل نقطة اختلاف أخرى عن الميكانيك الكلاسيكي وهي نظرية "عدم الاستنساخ " تنص على أنه من غير الممكن استنتاج حالة كمية مجهولةومن غير الممكن استنساخ حالات كمية غير متعامدة وان كانت هذه الحالات معلومة والحالات الوحيدة التي يمكن استنساخها هي مجموعة معروفة من الأشعة المتعامدة[1.10.11.12.13].

II-4-2الترميز المكثف *(Dense coding)*

لم نرى حتى الآن تأثير التشابك على نقل المعلومات، في الحقيقة كل ما شهدناه حتى الآن أنه لافرق بين البت الكمي المتشابك والبت الكلاسيكي في كمية المعلومات التي يمكن أن ينقلها، لكن هذه ليست سوى بداية القصة، ففي العنصر السابق لم نستخدم التأثير الغريب الذي ينقله التشابك الكمي و العنصر الحالي جاء بالضبط لهذه الغاية.

سابقا رأينا أن التشابك الكمي ينقل تأثير فوق زمني بين عناصره حيث أن التأثير على احداهما سواء بعملية قياس أو عملية تحويل واحدي يؤثر على البقية بشكل آني، الأمر الساحر بشأن هذا التأثير الغريب هو أنه من الممكن استغلاله لنقل معلومتين كلاسيكيتين بواسطة بت كمي واحد فقط ! تدعى هذه العملية بالترميز المكثف وهو بروتكول معين يسمح بنقل معلومتين ببت كمي واحد مستفيدا من ظاهرة التشابك الكمي.

نفترض أن اليس (Alice) حضر زوج من EPR الحالة $|\phi\rangle^+$ واحتفظ ببت كمي واحد وأرسل الأخر في رحلة بعيدة الى وحهة محددة عند المستقبلBob، قرر هذا المستقبل فجأة أن يرسل رسالة من اثنين من البت الكلاسيكي الى من أرسل اليه البت الكمي ، وليس لديه من وسيلة اتصال سوى القناة الكمية التي وصله البت الكمي عبرها وليس لديه أي بت كمي سوى ذاك الذي أرسل اليه .المعلومتان اللتان يريد المستقبل ان ينقلها الى اليس لها اربع احتمالات {|11⟩ .|10⟩ .|01⟩ .|00⟩} وله ان يستخدم أي تاثير واحدي على البت الكمي الذي لديه ، وهنا تلمع عبقرية .صحيح أنه ليس لديه سوى بت كمي واحد

لكنه في الواقع يستطيع التأثير على اثنين منهما بفضل التشابك الكمي، الأمر هنا أنه لايستطيع استخدام بت التكافؤ والطور للحالة المتشابكة حيث :

$$\begin{aligned} 00 &\rightarrow |\phi\rangle^{+} \\ 01 &\rightarrow |\phi\rangle^{-} \\ 10 &\rightarrow |\psi\rangle^{+} \\ 11 &\rightarrow |\psi\rangle^{-} \end{aligned} \qquad (40.\text{II})$$

لنقل رسالته الى اليس (المرسل) يطبق بوب (المستقبل) المؤثر المناسب على البت الكمي الذي لديه قبل يعيده مجددا الى المرسل(اليس) :

$$\begin{aligned} 00&: I\,|\phi\rangle^{+} = |\phi\rangle^{+} \\ 01&: \sigma_z\,|\phi\rangle^{-} = |\phi\rangle^{-} \\ 10&: \sigma_x\,|\psi\rangle^{+} = |\psi\rangle^{+} \\ 11&: \sigma_y\,|\psi\rangle^{-} = -i|\psi\rangle^{-} \end{aligned} \qquad (41.\text{II})$$

اذا عندما يعود البت الكمي الى المرسل من جديد يقوم بقياس ثنائية البت الكمي المتشابك التي لديه وفق الأساس:(34.II) ليتعرف على رسالة المستقبل، وبهذا يكون المستقبل قد استطاع تحميل بت كمي واحد بمعلومتين.[1.10.11.14]

لكن من المهم ألا نغفل نقطة مهمة هنا وهي أن نقل الرسالة بمعلومتين بواسطة عملية الترميز المكثف يحتاج الى اثنين من البت الكمي رغم أن المستقبل لم يستخدم سوى بت كمي واحد، وعذا راجع الى قدرته على التأثير على البت الكمي الآخر بفضل التشابك الكمي .للوهلة الأولى قد تبدو عملية الترميز

المكثف كما لو كنت في حاجة الى اثنين من البت الكمي لإرسال معلومتين لكن ما عليك سوى نقل بت كمي واحد، غير أن الحقيقة هي أن عملية النقل قد تمت مرتين بالفعل المرة الأولى كانت عند ارسال البت الكمي الى بوب (المستقبل) والثانية عند اعادته الى اليس (المرسل)، لكن الأمر الاستثنائي هنا هو أن عملية النقل الأولى لا تحمل أي معلومة في حين تحمل عملية النقل الثانية معلومتين في نفس الوقت.

II-4-3.النقل الكمي *(Quantum Teleportation)*

عندما تسمع جملة "النقل الكمي " قد يخطر ببالك أن الموضوع يتعلق بنقل نظام كمي ما، لكن الموضوع في الحقية هو عبارة عن نقل حالة كمية مجهولة لبت كمي دون نقل البت الكمي نفسه قد يبدو الأمر هنا وكأنه يخالف نظرية عدم الاستنساخ ولكن الحالة الكمية المجهولة تنقل ولا تستنسخ ، بمعنى أننا نأخذ حالة كمية مجهولة لبت كمي ثم ننقل هذه الحالة الى لبت كمي جديد موجود في مكان آخر ،وعملية النقل هذه تنشئ حالة لبت الكمي الأول ، أي ان الحالة الكمية المجهولة تختفي من مكان لتظهر في مكان آخر دون أن تكون هناك أي نسختان منها في أي وقت ، لذا لا يتعارض مع نظيره عند الاستنساخ .

النقل الكمي هو تطبيق مهم من تطبيقات التشابك الكمي، وبفضل الأثير الغريب الذي يظهره يمكن من نقل الحالة المجهولة لبت الكمي دون تميزيها . بروتوكول هذه العملية يبدأ بتشارك الحالة الكمية المتشابكة $|\phi\rangle^+_{AB}$ بين طرفين هما المرسل Alice والمستقبل Bob ، البت الكمي ذو الحالة المجهولة $|\varphi\rangle_C$ موجود لدى المرسل أي:

$$|\varphi\rangle_C = a|0\rangle_c + b|1\rangle_c$$

المرسل يريد نقل الحالة الكمية $|\varphi\rangle_C$ الى المستقبل لكن البت الكمي C ليس متشابكا مع البت الكمي الذي لدى المستقبل، لذا سيكون هدف المرسل هو إيجاد عملية مناسبة يمكنه من خلالها نقل الحالةالى $|\varphi\rangle_C$ المستقبل مستغلا البت الكمي المتشابك B الذي بحوزته ، البداية ستكون من خلال كتابة شعاع الحالة لثلاثتهم:

$$|\varphi\rangle_C|\phi\rangle^+_{AB} = \frac{1}{\sqrt{2}}\big((a|0\rangle_C + b|1\rangle_C)(|00\rangle_{AB} + |11\rangle_{AB})\big)$$

$$= \frac{1}{\sqrt{2}}(a|000\rangle_{CAB} + b|100\rangle_{CAB} + a|011\rangle_{CAB} + b|111\rangle_{CAB} \qquad (42.II)$$

الهدف الآن هو نقل المعاملات(a, b)الى اشعة البت الكمي B الموجود لدى المستقبل ومن أجل هذه الغاية نعيد كتابة أشعة الأساس غير متشابك لثنائي البت الكمي Aو C

(43.II)

$$|\psi\rangle_C|\phi\rangle^+_{AB} = \frac{1}{2}\big(a(|\phi\rangle^+_{CA} + |\phi\rangle^-_{CA})|0\rangle_B + b(|\psi\rangle^+_{CA} - |\psi\rangle^-_{CA})|0\rangle_B + a(|\psi\rangle^+_{CA} + |\psi\rangle^-_{CA})|1\rangle_B + b(|\phi\rangle^+_{CA} - |\phi\rangle^-_{CA})|1\rangle_B\big)$$

$$= \frac{1}{2}\Big(|\phi\rangle^+_{AC}(a|0\rangle_B + b|1\rangle_B) + |\phi\rangle^-_{AC}(a|0\rangle_B - b|1\rangle_B) + |\psi\rangle^+_{AC}(b|0\rangle_B + a|1\rangle_B) + |\psi\rangle^-_{AC}(-b|0\rangle_B + a|1\rangle_B)\Big)$$

$$|\varphi\rangle_C|\phi\rangle^+_{AB} = \frac{1}{2}|\phi\rangle^+_{CA}|\varphi\rangle_B + \frac{1}{2}|\phi\rangle^-_{CA}\sigma_z|\varphi\rangle_B + \frac{1}{2}|\psi\rangle^+_{CA}\sigma_x|\varphi\rangle_B + \frac{1}{2}|\psi\rangle^-_{CA}\mathrm{i}\sigma_y|\varphi\rangle_B$$

اذا لينقل المرسل الحالة الكمية $|\varphi\rangle$للبت الكمي C الى البت الكميB الموجود عند المستقبل عليه ان يقوم بقياس البت الكمي A وB وفق الأساس .هذا يؤدي الى انهيار شعاع الحالة لثلاثة البت الكمي الى احد اشعة المجموع في المعادلة السابقة .وعليه ينهار شعاع موجة البت الكميB الى احد الاشعة الأربعة $\{|\varphi\rangle_B, \sigma_x|\varphi\rangle_B, \mathrm{i}\sigma_y|\varphi\rangle_B, \sigma_z|\varphi\rangle_B\}$ وبالتالي عندما يحصل المرسل على نتيجة $|\phi\rangle^+_{CA}$ فالبت الكميB هو بالفعل في الحالة $|\varphi\rangle$.اما ان حصل على نتيجة أخرى فشعاع البت الكمي B ليس في الحالة $|\varphi\rangle_B$ بالضبط ولكن هو الشعاع $|\varphi\rangle_B$ بعد التأثير عليه بأحد مصفوفات باولي الثلاثة اذا ليحصل المستقبل على الشعاع $|\varphi\rangle_B$عليه ان يطبق مقلوبها على البت الكمي B وبما اننا نعلم ان هذه المؤثرات واحدية و هرميتيه فكل ما على المستقبل فعله هو ان يعيد تطبيق المؤثر نفسه على شعاع حالة البت الكمي B.الجدول **(2.II)** يوضح التحويل الذي يجب على المستقبل تطبيقه من اجل الحصول على شعاع الحالة $|\varphi\rangle_B$ حسب النتيجة التي تحصل عليها المرسل .

الجد ول (2.II) يوضح جميع المتعلقة بالنقل جدول الكمي ونتائجه العمليات

نتيجة قياس المرسل	شعاع البت الكمي B	عملية التحويل على البت الكمي B	شعاع البت الكمي Bالجديد
$\|\phi\rangle^{+}_{CA}$	$a\|0\rangle_B+b\|1\rangle_B$	I	$a\|0\rangle_B+b\|1\rangle_B$
$\|\phi\rangle^{-}_{CA}$	$a\|0\rangle_B-b\|1\rangle_B$	σ_z	$a\|0\rangle_B+b\|1\rangle_B$
$\|\psi\rangle^{+}_{CA}$	$b\|0\rangle_B+a\|1\rangle_B$	σ_x	$a\|0\rangle_B+b\|1\rangle_B$
$\|\psi\rangle^{-}_{CA}$	$-b\|0\rangle_B+a\|1\rangle_B$	σ_y	$e^{i\frac{\pi}{2}}(a\|0\rangle_B+b\|1\rangle_B)$

العملية التي على المستقبل ان يطبقها حتى يتم نقل الحالة الكمية $|\varphi\rangle$ من المرسل الى المستقبل تعتمد على نتيجة قياس المرسل. اذا يبقى المستقبل في انتظار اتصال المرسل ليخبره بنتيجة قياسه حتى يعلم أي تحويل عليه القيام به لنقل تلك الحالة ، وهو مايتفق مع النظرية النسبية الخاصة ،فلا يمكن ان يتم نقل المعلومات او طاقة بسرعة اكبر من سرعة الضوء لاحظ أيضا ان عملية النقل للحالة المجهولة تمت بدون ان يتم معرفة أي شيء عنها ، فالنتيجة التي يتحصل عليها المرسل لا تتعلق باي شكل من الاشكال بالحالة المجهولة $|\varphi\rangle$ اوالا كان هذا متناقضا مع نظرية عدم الاستنساخ ، لذا من المهم هنا تجديد التأكيد على ان الذي حدث هو عملية نقل وليس عملية نسخ .[10.15.16].

II-4-4 توزيع المفتاح الكومي*(Quantum Key Distribution)*

تعتمد معظم أنظمة الاتصال اليوم نوعا معينا من التشفير، قد لا تنبه لهذا لكن انتقال المعلومات في أي جهاز اتصال يستخدم عملية تشفير معينة حتى تنتقل المعلومة من اللغة البشرية العادية الى لغة الآلة ليتمكن الجهاز فيما بعد من نقلها أو تخزينها.

علم التشفير' cryptography' يهدف في الأساس لإخفاء المعلومات أو البيانات عن طريق استخدام شيفرة سرية تجعل من تلك البيانات أو المعلومات غير مفهومة لغير من يملك تلك الشيفرة. ان نقل المعلومات بسرية يتطلب وجود شيفرات خاصة وبروتوكولات معينة لتحقيق نقل آمن للمعلومات، لكن كلما تطورت عمليات التشفير تطور معها جانبا الى جنب علم تحليل الشفرات' cryptanalysis'، والذي يطرح خطرا دائما بأن اكتشاف الرسالة السرية بواسطة جاسوس أو متلصص ما، لكن هناك نوعا محدد من عمليات التشفير – ان هو طبق بنجاح – تكون عملية اختراق الرسالة المشفرة بواسطته غير ممكنة على الاطلاق!

تدعى هذه الطريقة بالمفتاح السري' Privatekey' المميز في طريقة المفتاح السري أن الرسالة المشفرة التي تنتقل بين مستخدمين لا تحمل بمفردها أي معلومة على الاطلاق ولايمكن لمن يحصل عليها أن يكتشف الرسالة السرية التي تنقلها. السر في هذه الطريقة يمكن في المفتاح السري الذي يكون موجودا لدى المستخدمين فقط وغير معروف لأي أحد سواهما

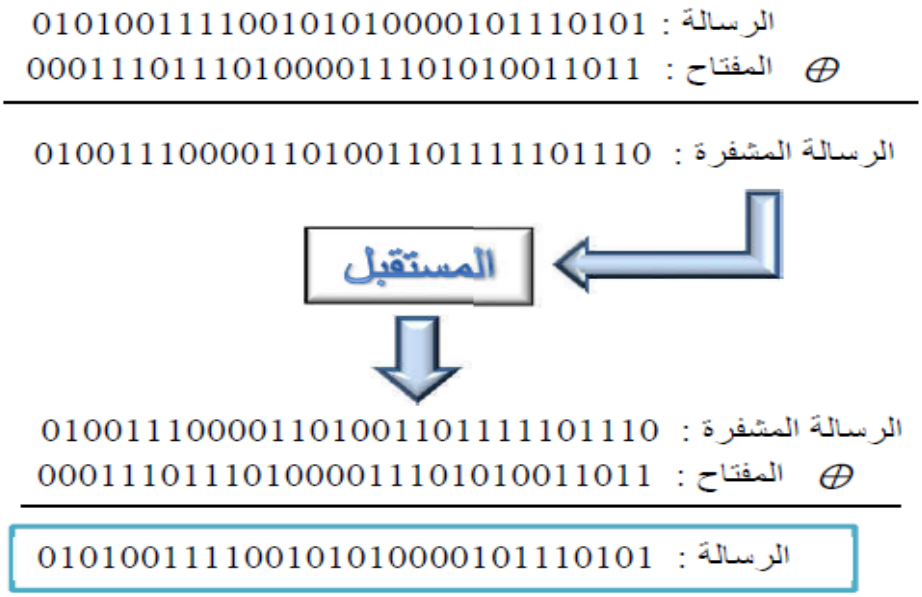
لنقل الرسالة بطريقة المفتاح السري تحول أولا الى النظام الثنائي (0.1) بواسطة نظام ترميز معروف كلغةASCII مثلا ثم يضاف اليها المفتاح والذي يكون عبارة عن سلسلة من رقمين (0.1) على ان يكون طوله مساويا لطول الريالة على الأقل يجمع كل رقم من الرسالة مع المفتاح على ان يكون الجمع بباقي القسمة على اثنين (النتيجة هي باقي قسمة المجموع على الرقم اثنين) ثم ترسل السلسة المتحصل عليها الى الوجهة المطلوبة ، والتي كل ما عليها القيام به هو إضافة المفتاح من جديد الى السلسة لتتحصل على

الرسالة السرية (من جديد الجمع يكون بباقي القسمة على اثنين) مثال يصور هذه الطريقة موجود في الحالة القصوى المتشابكة لاثنين من البت الكمي

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(a|00\rangle_{AB} + b|11\rangle_{AB})$$

نقطة القوة لهذه الطريقة هو أنه لا يمكن اكتشاف الرسالة من دون وجود المفتاح ، بل انه يمكنك حتى من الرسالة تعطي نسخة من الرسالة المشفرة الى المتلصص من دون أن يستطيع أن يفكها ، لأنها بالفعل سلسة عشوائية تماما ولا تحمل أي معلومة يمكن للمتلصص أن يستغلها ، فنفس الحرف في الرسالة يشفر بتتابع مختلف من الرقمين 0 و 1 في كل مرة حسب موضعه وتتابع الأرقام في المفتاح في تلك المنطقة هذه الطريقة آمنة تماما اذا لأن احتمال ان يكشف المتلصص الشيفرة قبل الحصول على نسخة من الرسالة المشفرة مساو لاحتمال أن يكشفها بعد أن حصل على نسخة من الرسالة[16.17.18]

يبدو أن كل شيء ممتاز لحد الساعة، الطريقة آمنة جدا وغير قابلة للاختراق ان تم تشارك مفتاح سري بين المستخدمين بسرية وأمان، وهنا يظهر أكبر عائق هلمي امام هذا البروتوكول: فكيف يمكن ان يتم تشارك المفتاح بطريقة سرية؟ يظهر هنا وكأن علينا العودة لطرق التشفير الأخرى لنقل المفتاح بسرية ونكون هكذا قد عدنا بالفعل الى نقطة الصفر، لأن أمان المفتاح السري هنا سيعتمد على مخطط لمثال يوضح مبدأ عمل التشفير بواسطة المفتاح الخاص ' Private Key'



(8-II) مخطط لمثال يوضح مبدأ عمل التشفير بواسطة المفتاح الخاص 'Private Key'

قد تتم مشاركة المفتاح يدا بيد بين المستخدمين لكن هذا ليس عمليا بالمرة، واستخدام وسيط لينقل المفتاح يزيد من مخاطر أن يكتشف فكلما زادت الأطراف المشاركة في العملية التشفير زاد خطر الاختراق، ما العمل إذا؟ ربما قد تكون الفكرة قد لمعت في رأسك بالفعل، يمكن استخدام التشابك الكمي لتشارك مفتاح سري عن طريق قياس مجموعة من الأجسام المتشابكة المشتركة بين المرسل والمستقبل بالفعل يمكن للتشابك الكمي ان يمهد طريقا امنة لنقل المفتاح بكل أمان لتوضيح الطريقة المتبعة لنقل المفتاح بواسطة التشابك الكمي بشكل عملي نتبع البروتوكول التالي:

يتشارك المستخدمان حالة متشابكة معينة كأن يحضر المرسل مثلا مجموعة من ثنائيات البت الكمي في الحالة المتشابكة $|\psi^-\rangle$ ثم يقوم بأرسال بت كمي من كل ثنائيات متشابكة نحو المستقبل. بعد اكتمال عملية الارسال يقوم كل من المرسل والمستقبل بقياس كل بت كمي متشابك من مجموعة وفق أساس الملاحظ S_x

او الملاحظ S_x بشكل عشوائي، على ان يحاولا ان تكون العملية متوازنة في النهاية بحيث حوالي نصف عمليات القياس تكون للملاحظ S_z والنصف الاخر للملاحظ S_x

عمليات القياس تتم بشكل منفصل و دون ان يخبر أحد المستخدمين الاخر عن الملاحظ الذي سيقوم بقياسه لكل بت كمي حتى تنتهي جميع عمليات القياس لعناصر المجموعة، عندها يقوم كل المرسل والمستقبل بالإعلان عن الملاحظ الذي قاما بقياسه لكل بت كمي دون الإفصاح عن نتيجة القياس. الإعلان يتم عبر قناة اتصال كلاسيكية وليس على هذه القناة ان تكون امنة، فالتواصل بين المستخدمين الذي يتم عبر هذه القناة لا يحمل أي معلومات من الممكن ان يستفيد منها المتلصص لأن المعلومات كامنة في التشابك والترابط الذي يكون بين عناصره.

بعد معرفة كل مستخدم ل لملاحظات التي قاسها المستخدم الاخر اصبح من الممكن استخراج سلسلة المفتاح من نتائج القياس، فعندما يجد المستخدمان انهما قد قاسا نفس الملاحظ لنفس البت الكمي فالنتيجة التي حصلا عليها مترابطة بفضل التشابك الكمي ،ويكونان قد حصلا على عنصر من سلسلة المفتاح السري .أما ان قاما بقياس ملاحظين مختلفين لنفس ثنائية البت الكمي فنتيجتا القياس غير مترابطين وبالتالي لن تشكلا جزءا من المفتاح .على العموم تكون نتيجتا المرسل والمستقبل مترابطتين في نصف الحالات تقريبا، الاتفاق عبر الرقمين 0 و 1بنتيجة قياس كل منهما .تدعى عملية توليد المفتاح السري بالطريقة السابقة ببروتوكول EPR، والأمر المثير المتعلق به هو ان المستخدمين يمكنهما الا يقوما بعملية القياس الا عند الحاجة لنقل رسالة بينهما ، عندها فقط تتم عملية القياس و توليد المفتاح السري .

بروتوكول EPR ليس بالطريقة الوحيدة لنقل المفتاح السري باستخدام التشابك الكمي فثمة بروتوكول يستعان يه هو الاخر لنقل المفتاح ويدعى بمعكوس EPR (time-Reversed EPR)، وكما يوحي الاسم يقوم المستخدمان بالخطوات المعاكسة لتجربة EPR.

II-4-5 متلصص في الجوار

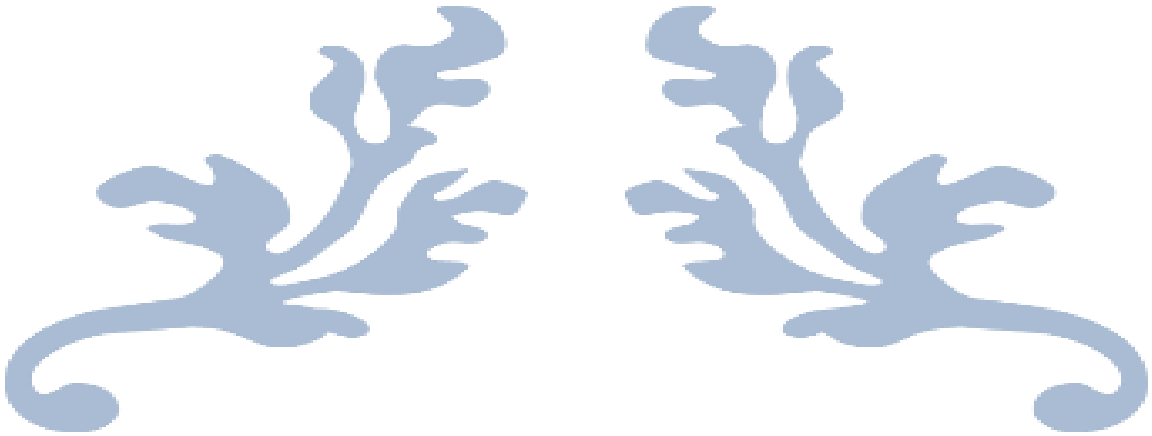
البروتوكولات التي تم استعراضها في العنصر السابق قادرة على نقل المفتاح السري بالاعتماد على ميكانيك الكم، لكن يبقى هناك تساؤل مشروع وهو هل هذه الطريقة امنة تماما؟ فقد يختبأ متلصص في الجوار يبحث عن فرصة ليكتشف المفتاح، قد يتلصص على القناة الكلاسيكية للمستخدمين لكن المعلومات المنتقلة في تلك القناة لن تمكنه من معرفة المفتاح لأن نقل المفتاح يتم في القناة الكمية، ما يعني انه مضطر الى التجسس على القناة الكمية التي تنقل البت الكمي.

وحسب نظرية عدم الاستنساخ لا يمكن للمتلصص ان يتعرف على حالة البت الكمي من دون ان يؤثر عليها، وذلك لأنه يحاول التعرف على حالتين كميتين غير متعامدتين، وبالتالي فان تأثيره على حالة البت الكمي المار بالقناة الكمية سيفيد الترابط الذي ينبغي ان يكون بين نتائج المستخدمين، ما يعني انه يمكن كشف المتلصص عند المقارنة العلنية للأجزاء محدودة من المفتاح اذا تضمن نظرية عدم الاستنساخ في هذه الحالة ام يكون فعل المتلصص قابلا للرصد

في بروتوكولEPR الاعتماد يكون على التشابك الكمي اين تكوم الحالة الكمية لثنائية البهت الكمي المتشابكة معروفة، قد يحاول المتلصص في هذه الحال ان يشابك الحالة لثنائية البت الكمي مع بت كمي اخر بحوزته عن طريق التأثير على البت الكمي المتنقل داخل القناة، لتصبح الحالة الكلية لثلاثية البت الكمي من الشكل:

$$|S\rangle_{ABE} = |00\rangle_{AB} \, |e_{00}\rangle_E + |01\rangle_{AB} \, |e_{01}\rangle_E + |10\rangle_{AB} \, |e_{10}\rangle_E + |11\rangle_{AB} \, |e_{11}\rangle_E$$

الاشعة التي تحمل الدليل E هي اشعة خاصة بالبت الكمي للمتلصص لاحظ ان المتلصص صار بإمكانه التعرف على نتيجة قياس المستخدمين، لأن عملية القياس هاته ستؤدي الى انهيار حالة البت الكمي الذي لديه شعاع محدد، وبعد اعلان المستخدمين للملاحظات التي قاموا بقياسها يمكن للمتلصص ان يقوم بقياس الأساس المناسب للبت الكمي الذي لديه ليتعرف على نتيجة قياس المستخدمين[16].



الفصل الثالث
الخوارزميات الكمومية

III.1.تمهيد

الخوارزميات الكلاسيكية المستعملة في الحواسيب الحديثة تستعمل المنطق الكلاسيكي . مؤخرا بدأ الباحثون بإستعمال التصرفات الكمومية كأساس لمنطق كمومي شديد تبنى عليه خوارزميات تسمى الخوارزميات الكمومية والتي عبارة عن تطبيق بوابات كمومية لغرض معين. وهي عملية وحدوية تحول مجموعة من الكيوبيتات كمدخل الى مجموعة من الكيوبيتات يتم قراءتها وفق للعملية الوحدوية وتكون نتائج قراءة المخرجات حسب هدف معين . من أهم الخورزميات وأشهرها Deutsch-Jozsa , simon algorithme algorithm وفي مذكرتنا هذه ندرس خوارزمية grover algorithme.

III.2.شرح بعض الخوارزميات

III.1.2.خوارزمية"Deutsch " :

مشكلة **'Deutsch'**عبارة عن صندوق أسود يقوم بوظيفة بسيطة في النظام الكلاسيكي بحيث تكون المدخلات اثنين بت وتنتج اثنين بت أي عدد المدخلات والمخرجات متساوي .هذه الخوارزمية لها أربع دوال بالضبط كما هو موضح في الجدول (III.1) التالي:

الدالة	$f(0)$	$f(1)$
f_0	0	0
f_1	0	1
f_2	1	0
f_3	1	1

الجدول(III.1): جدول يوضح دوال خوارزمية"**Deutsch** "

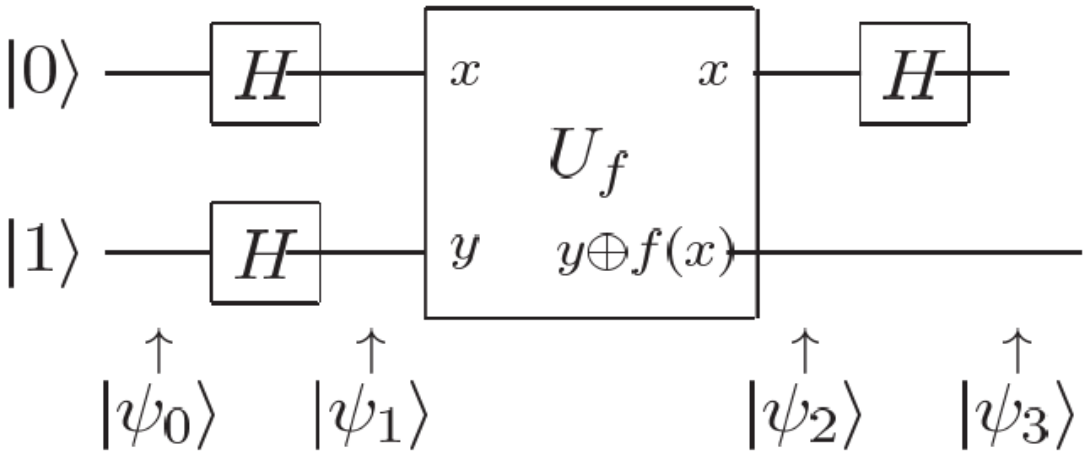
الحالة الأولى:f_0وf_3تسمى دالة ثابتة فهي لا تغير قيمة المدخلات تحافظ على نفس القيمة

الحالة الثانية: f_1و f_2 تسمى دالة متوازنة تقوم بتغير قيمة المدخلات اذا كان بت 0 تحوله الى 1 والعكس صحيح، هدف مشكلة دوتش يتمثل في التميز بين الدوال الحالة الأولى والثانية ، في النظام الكمومي نستطيع تحديد ما اذا كانت ثابتة أو متوازنة بواسطة بت كمي واحد فقط. في عام 1985 عندما جاء دوتش بهذه الخوارزمية كان لديه نسخة منها معدلة قليلا ، الخوارزمية تصف

الجملة الكمومية التالية "نظرية التعقيد كانت تهتم بشكل رئيسي بالقيود على حساب الدوال " أي يمكن حساب الدوال بسرعة مع أجهزة الكمومية باستخدام بت كمي واحد فقط بدلا من الحواسب الكلاسيكية نحتاج الاثنين بت كلاسيكي تمكن هذه الخوارزمية الحد الأدنى للوقت الحسابي لبعض المهام [4.19].

III. 1.1.2.مخطط خوارزمية'Deutsch'

$$\text{QuantumOraclef: } \{0,1\}^n \rightarrow \{0,1\}$$



الرسم التخطيطي(**1.** III): رسم تخطيطي يوضح خوارزمية Deutsch.

III.2.1.2 شرح الخوارزمية:

أولا: نقوم بإدخال كوبتين أحدهما في الحالة⟨0 اوالأخر في الحالة⟨1 ا

$$|\psi_0\rangle = |01\rangle \qquad (1.\text{III})$$

ثانيا: نطبق بوابة الهاد مارH على كل من الحالتين نجد :

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \qquad (2.\text{III})$$

نضع $f(x) = 0$أي

$$y \oplus f(x) = y \oplus 0 = \frac{1}{\sqrt{2}}(|0 \oplus 0\rangle-|1 \oplus 0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

نضع $f(x) = 1$أي

$$y \oplus f(x) = y \oplus 1 = \frac{1}{\sqrt{2}}(|0 \oplus 1\rangle - |1 \oplus 1\rangle) = \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle)$$

بالتعميم نتحصل على

$$y \oplus f(x) = \frac{1}{\sqrt{2}}(-1)^{f(x)}(|0\rangle - |1\rangle)$$

ثالثا: نطبق تحويل $u_f|\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle$;

$$(-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad (3.\text{III})$$

يمكننا القول أن:

$$u_f\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right]$$

$$= \frac{1}{2}\left[(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)\right]$$

عندما تكون f ثابتة أي $f(0) = f(1)$

$$|\psi_2\rangle = \frac{1}{2}\left[(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)\right]$$

$$|\psi_2\rangle = \frac{1}{2}(-1)^{f(0)}[|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)]$$

$$|\psi_2\rangle = \pm\frac{1}{2}[|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)]$$

عندما تكون f ثابتة أي $f(0) \neq f(1)$

$$|\psi_2\rangle = \frac{1}{2}\left[(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)\right]$$

$$|\psi_2\rangle = \frac{1}{2}\left[(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1) * (-1)^{f(0)}|1\rangle(|0\rangle - |1\rangle)\right]$$

$$|\psi_2\rangle = \frac{1}{2}(-1)^{f(0)}[|0\rangle(|0\rangle - |1\rangle) - |1\rangle(|0\rangle - |1\rangle)]$$

$$|\psi_2\rangle = \pm\frac{1}{2}[|0\rangle(|0\rangle - |1\rangle) - |1\rangle(|0\rangle - |1\rangle)]$$

$$|\psi_2\rangle = \begin{cases} \mp\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \\ \mp\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \end{cases} \qquad (4.\text{III})$$

رابعا: نطبق الهاد مارد H على$|0\rangle$ فقط

$$|\psi_3\rangle = \begin{cases} \mp\frac{1}{\sqrt{2}}|0\rangle(|0\rangle-|1\rangle) iff(0) = f(1) \\ \mp\frac{1}{\sqrt{2}}|1\rangle(|0\rangle-|1\rangle) iff(0) \neq f(1) \end{cases} \qquad (5.\text{III})$$

$$f(0) \oplus f(1) = 0 \Leftrightarrow f(0) = f(1)$$

$$|\psi_4\rangle = \pm f(0) \oplus f(1)\left[\frac{|0\rangle + 1\rangle}{\sqrt{2}}\right] \qquad (6.\text{III})$$

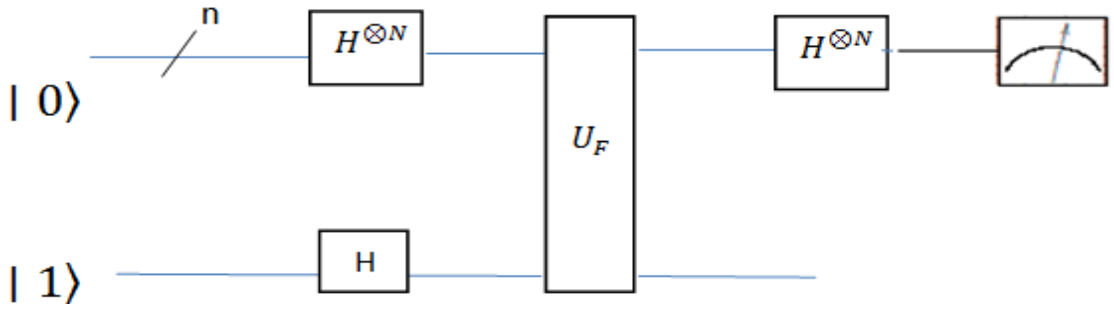
III.2.2.خوارزمية "Deutsch-Jozsa "

خوارزمية "Deutsch−Jozsa" هي ببساطة تعميم متعدد النقاط لخوارزمية"Deutsch".

يعطي هذا الإجراء طريقة لتقرير ما إذا كان تطبيق$\{0,1\}^n \to \{0,1\}: f$ ثابتا أو متزنا[1]

لنفترض أننا نعلم مسبقا أن f إما ثابة وإما متزنة، كلاسيكيا لمعرفة طبيعة f (ثابتة بالضبط أو متزنة باضبط) يجب إجراء $\frac{2^n}{2}+1$ عملية، الإجراء الكمومي يسمح بمعرفة طبيعة f بعملية واحدة.

III.2.2. 1. مخطط خوارزمية "Deutsch-Jozsa"



الرسم التخطيطي (**2.** III): رسم تخطيطي يوضح خوارزمية Deutsch-Jozsa.

III.2.2. 2. شرح الخوارزمية:

الترميز $|0\rangle^{\otimes N}$ يعني n−qbit متساوي في نفس الحالة صفر

أولا: نحضر $|0\rangle^{\otimes N}$

$$|\psi_0\rangle = |0\rangle^{\otimes N}|1\rangle = |00\ldots\ldots0\rangle|1\rangle \qquad (III.7)$$

ثانيا: نطبق عليها $H^{\otimes N}$

بعد التحويل ينتج عن كل كوبت حالة تراكب أي مزج من كوبتين

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle(|0\rangle - |1\rangle) \qquad (8.III)$$

ثالثا: نطبق عملية u_f، حيث : u_fعملية كمومية

$$u_f|x\rangle|y\rangle \rightarrow |x\rangle|y\oplus f(x)\rangle \rightarrow \frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x\rangle(|f(x)\rangle - |1\oplus f(x)\rangle)$$

$$\forall x, \qquad f(x) = 0 \text{أو} 1$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \qquad (9.III)$$

بينما الكيوبت الأخير في حالة $|1\rangle$ بعد أن نطبق عليه الهادمارد ينتج

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

في الأخير تعطى كوبت على النحو التالي :

$$|\psi_3\rangle = \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\sum_{y=0}^{2^n-1}(-1)^{x.y}|y\rangle$$

$$|\psi_3\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\left(\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x.y}\right)|y\rangle \qquad (10.III)$$

x.y = $x_0y_0 \oplus x_1y_1 \oplus \ldots\ldots\ldots\ldots\ldots x_ny_n$ تكون البت من أجزاء بتات أخرى

بعد القياس اذا وجد الاحتمال $|0\rangle^{\otimes n}$ هو 1 يعني نتيجة التداخل(بناء) أي f(x)ثابتة (constante)، اذ وجد الاحتمال هو 0 أي نتيجة التداخل(هدام) فان f(x)متوازنة (balance) .[19].

III.3.2.خوارزمية"Simon's algorithm"

$$f: \{0,1\}^n \rightarrow \{0,1\}^n$$

مشكلة **Simon** يتم إعطاء دالة من سلاسل لها n−bit الى سلاسل n−bit بحيث يوجد s يحقق

$\exists\, s \in \{0,1\}^n$ يحقق[20]

$$f(x) = f(y) \Leftrightarrow x \oplus y \in \{0^n, s\}, \text{si} \quad s = 0^n.$$

الهدف هو إيجاد s. (شرط $s = 0^n$ اذن تقابلي)

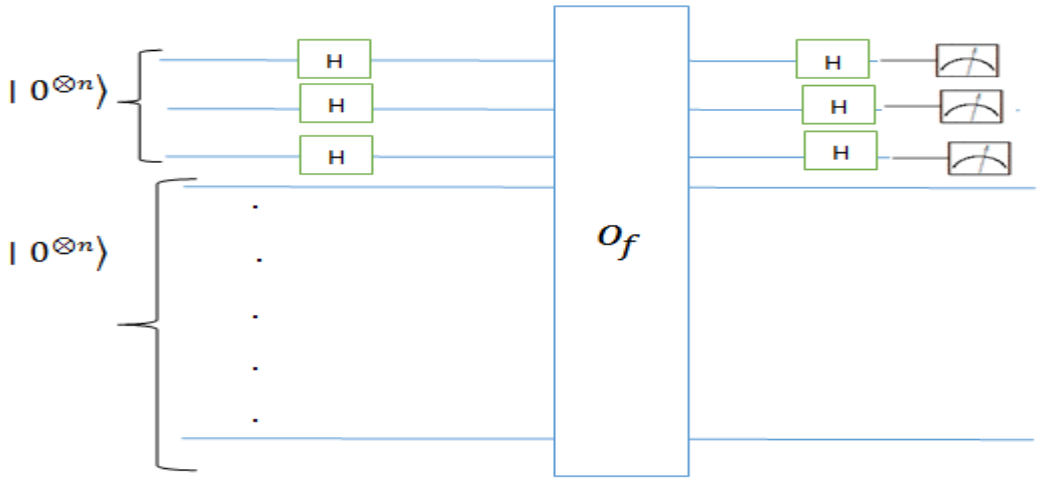
لنأخذ مثالا للتوضيح : n=3

الدالة F تحقق الخصائص

X	F(x)
000	101
001	010
010	000
011	110
100	000
101	110
110	101
111	010

الجدول(III .2): يوضح الحالة الكلاسيكية للبحث عن x. y من أجل f(x)=f(y)

III.3.2. 1.مخطط خوارزمية سايمون Simon's algorithm



الرسم التخطيطي(III .3): رسم تخطيطي يوضح خوارزمية**Simon.**

III.3.2. 2.شرح الخوارزمية:

لاحظ أنه عند تطبيق $H^{\otimes n}$ تكتب بالشكل التالي:

$$H^{\otimes n}\,|\,x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x.y}\,|\,y\rangle$$

أولا: ندخل كيوبيتات في الحالة

$$|\,\psi_0\rangle = |\,0^{\otimes n}\rangle|\,0^{\otimes n}\rangle \qquad (11.\,\mathrm{III})$$

ثانيا: نطبق الهادامارد H على كوبيتات الجزء الأول.

$$|\,\psi_0\rangle = |\,0^{\otimes n}\rangle|\,0^{\otimes n}\rangle \rightarrow Hadamard$$

$$|\,\psi_1\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|\,x\rangle|\,0^n\rangle \qquad (12.\,\mathrm{III})$$

ثالثا: نطبق O_f

$$|\,\psi_1\rangle \rightarrow O_f$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle \qquad (13.\text{III})$$

ثالثا: نطبق الهادامارد H على كوبيتات الجزء الأول

$$|\psi_2\rangle \rightarrow Hadamard$$

$$|\psi_3\rangle = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}(-1)^{x.y}|y\rangle|f(x)\rangle$$

$$|\psi_3\rangle = \sum_y\left(\frac{1}{2^n}\sum_x(-1)^{x.y}|f(x)\rangle\right)|y\rangle \qquad (14.\text{III})$$

اذا كان $s = 0^n$ فان f تقابلي اذن الاحتمال يكون :

$$\left\|\sum_x(-1)^{x.y}|f(x)\rangle\right\|^2 = \frac{1}{2^n} \qquad (15.\text{III})$$

اذا كان $s \neq 0^n$ نكتب الاحتمال :

$$\left\|\sum_x(-1)^{x.y}|f(x)\rangle\right\|^2 = \begin{cases} 0 \\ 2^{-(n-1)} \end{cases} \qquad (16.\text{III})$$

النتيجة النهائية للاحتمال هي:

$$\mathrm{P(y)} = \left\|\sum_x(-1)^{x.y}|f(x)\rangle\right\|^2 \qquad (17.\text{III})$$

III .3. تقدير الطور (Phase estimation)

المسألة هي: $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$ نريد إيجاد تقدير لـ θ(phase estimation)

U: عبارة عن مصفوفة وحدوية[1]

$\{|\psi_1\rangle, \dots\dots\dots\dots\dots |\psi_n\rangle\}$ اشعة الأساس

$$\lambda_k = e^{i2\pi\theta}|\psi\rangle$$

الاشعة الذاتية تكون $\{|\psi_1\rangle, \dots\dots\dots\dots\dots |\psi_n\rangle\}$

$$\{e^{2\pi i\theta_k}; k = 1, \dots \dots 2^n\} \; ; \theta_k \in [0,1]$$

المشكلة :إيجاد تقدير الطور لθ

$$\begin{cases} U|\varphi_j\rangle = e^{2\pi i\theta_j} |\psi_j\rangle \\ U|\psi\rangle = e^{2\pi i\theta} |\psi\rangle \end{cases}$$

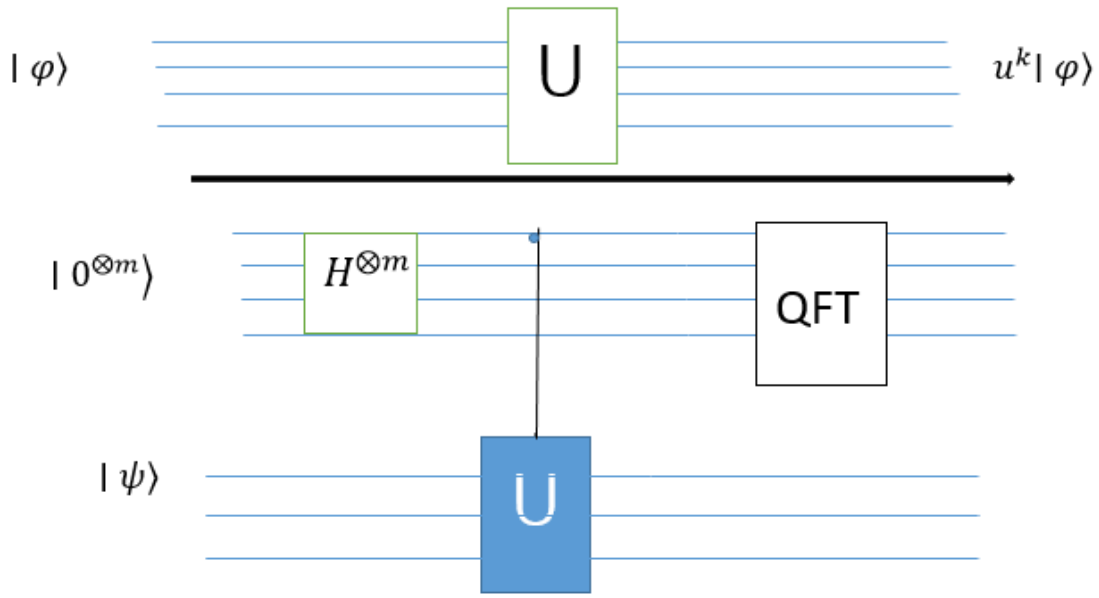
$\Lambda_m(u)$: تحويل وحدوي(m + n) على بت

$$U \rightarrow \Lambda_m(u)|k\rangle|\varphi\rangle = |k\rangle u^k|\varphi\rangle$$

بتk ∈ {0, … … . $2^m - 1$}et∀$|\varphi\rangle$

k: عدد مرات المطبقة

III .3. 1مخطط تقدير الطور(phase estimation): [1]



الرسم التخطيطي(**III .4**): رسم تخطيطي يوضح تقدير الطور.

III .3. 2. شرح المخطط:

أولا:ندخل

$$|\psi_0\rangle = |0^m\rangle|\psi\rangle \qquad (18.\text{III})$$

ثانيا:نطبق $|\psi_0\rangle \rightarrow$ Hadamar

$$|\psi_1\rangle = \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle |\psi\rangle \qquad (19.\text{III})$$

بعد $\Lambda_m(u)$

$$|\psi_2\rangle = \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle (u^k |\psi\rangle) \qquad (20.\text{III})$$

ثالثا :

$$u|\psi\rangle = e^{2\pi i\theta}|\psi\rangle \rightarrow u^k|\psi\rangle = e^{2\pi ik\theta}|\psi\rangle$$

ومنه

$$|\psi_3\rangle = \left(\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle e^{2\pi i\theta}\right)|\psi\rangle \qquad (21.\text{III})$$

نضع $\theta = \frac{j}{2^m}$ $\quad j \in \{0,1,\dots\dots\dots,2^m-1\}$

$$\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} e^{2\pi ikj/2^m} |k\rangle = \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} \left(e^{2\pi i/2^m}\right)^{kj} |k\rangle$$

$$|\psi_4\rangle = \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} (w)^{kj} |k\rangle \qquad (22.\text{III})$$

بحيث $w = \frac{2\pi i}{2^m}$

نضع $|\phi_j\rangle = \frac{1}{2^{\frac{m}{2}}} \sum_{k=0}^{2^m-1} (w)^{kj} |k\rangle$ اذن $|\phi_j\rangle$ يكون

$$J = \theta \Rightarrow \langle \varphi_j | \varphi_j \rangle = \delta_{jj'}$$

في الأخير $\exists F'; F'|j\rangle = |\phi_j\rangle$

$$F' = \frac{1}{\sqrt{2^m}}\begin{pmatrix} |\phi_0\rangle & |\phi_1\rangle & \end{pmatrix} = \mathrm{QFT}_{2^m} \qquad (23.\mathrm{III})$$

$$\mathrm{QFT}_{2^m}|\phi_j\rangle = \frac{1}{2^{m/2}}\sum_{k=0}^{\infty} e^{2\pi ijk/2^m}\ |k\rangle|j\rangle \qquad (24.\mathrm{III})$$

تطبيق QFT على qbit على الحالة: $\theta \neq \frac{j}{2^m}$

$$\frac{1}{2^{m/2}}\sum_{k=0}^{2^m-1}|k\rangle e^{2\pi ijk/2^m}\sum_{j=0}^{2^m-1}\left(\frac{1}{2^m}\sum_{k=0}^{2^m-1}e^{2\pi ik(\theta-\frac{j}{2^m})}\right)|j\rangle \qquad (25.\mathrm{III})$$

أخيرا نتحصل على الاحتمال

$$P_j = \left\|\frac{1}{2^m}\sum_{k=0}^{2^m-1}e^{2\pi ik\left(\theta-\frac{j}{2^m}\right)}\right\|^2 \qquad (26.\mathrm{III})$$

$$P_j{}^{\theta} = \frac{1}{2^m}\left\|\frac{e^{2\pi i(2^m\theta-j)}-1}{e^{2\pi i(\theta-\frac{j}{2^m})}-1}\right\|^2 \qquad (27.\mathrm{III})$$

III. 4.خوارزمية Grover

III.4.1 تعريف:هي البحث الغير مهيكل في قائمة غير منظمة .الخوارزمية تجعل استخدام n كيوبيت فردي صحيح مسجل[1].

الهدف من الخوارزمية هو إيجاد حل لمشكلة البحث الغير مهيكل، بإستخدام أصغر عدد ممكن من التطبيقات oracl [1].

يكتب : $\mathrm{Oracle}(z_f),(o_f)$ $f:\{0,1\}^n \to \{0,1\}$

$$O_f\,|x\rangle|a\rangle = |x\rangle|a\oplus f(x)\rangle \qquad (28.\mathrm{III})$$

$$x \in \{0,1\}^n \ \text{et}\ a \in \{0,1\}$$

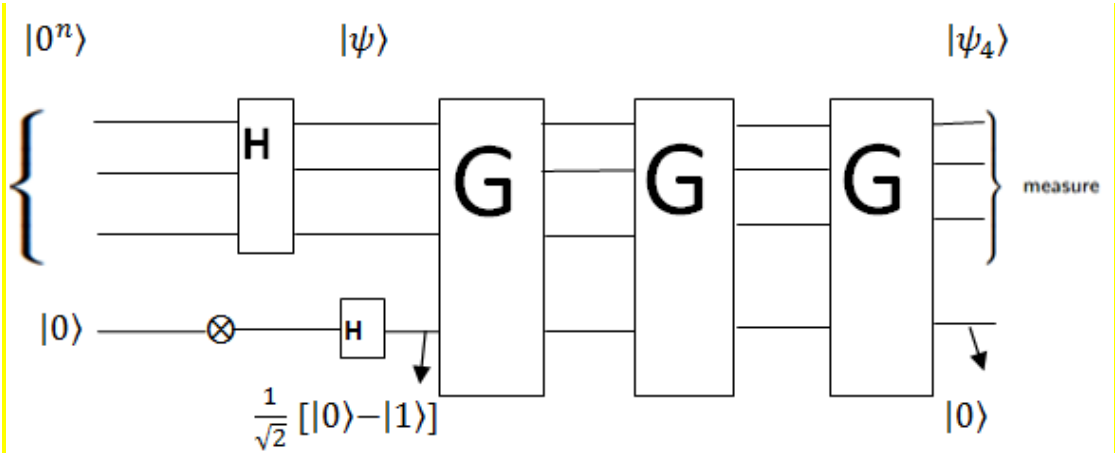
إيجاد $x \in \{0,1\}^n$ بحيث $f(x) = 1$,

نبحث على xبحيث $f(x) = 1$ أوإثبات أن x غير موجود.

$$z_f|x\rangle = (-1)^{f(x)}|x\rangle (29.\text{III}) Z_0|x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0^{\otimes n} \\ |x\rangle & \text{if } x \neq 0^{\otimes n} \end{cases} \text{ و} \qquad (30.\text{III})$$

$$x \in \{0,1\}^n \; ; \quad (Z_0 = \prod -2|0^n\rangle\langle 0^n|$$

4.III. 2.مخطط خوارزمية Grover: تكرار GroverK مرة



الرسم التخطيطي(5.III): رسم تخطيطي لخوارزمية البحث الكمي Grover.

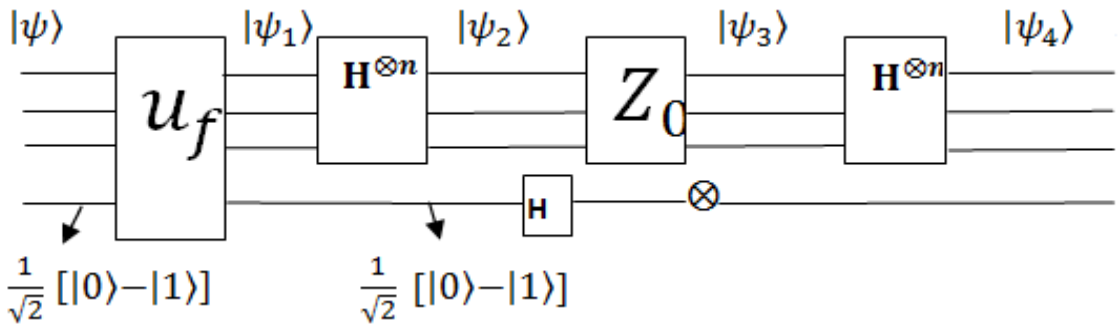
4.III. 3.شرح خوارزمية Grover

تحليل G:

$$\text{H}^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle = |\psi\rangle$$

نبرهن أن:

$$\text{G} = -\text{H}^{\otimes n} Z_0 \text{H}^{\otimes n} Z_f (31.\text{III})$$



الرسم التخطيطي(III.6): رسم تخطيطي لدائرة تكرار Grover.

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \qquad (32.\text{III})$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \qquad (33.\text{III})$$

$$|\psi_2\rangle = \mathrm{H}^{\otimes n} |\psi_1\rangle \qquad (34.\text{III})$$

$$= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{xy} |y\rangle$$

$$= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |0\rangle + \frac{1}{2^n} \sum_{x=0}^{2^n} (-1)^{f(x)} \sum_{y=1}^{2^n-1} (-1)^{xy} |y\rangle$$

$$|\psi_3\rangle = Z_0 |\psi_2\rangle (35.\text{III})$$

$$= \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f(x)} (-1)^{xy} Z_0 |y\rangle$$

$$= \frac{1}{2^n} \left(\sum_{x=0}^{2^n-1} (-1)^{f(x)} |0^n\rangle - \sum_{x=0}^{2^n-1} \sum_{y=1}^{2^n-1} (-1)^{f(x)} (-1)^{xy} |y\rangle \right)$$

$$= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |0\rangle - \frac{1}{2^n} \sum_{x=0}^{2^n} (-1)^{f(x)} \sum_{y=1}^{2^n-1} (-1)^{xy} |y\rangle$$

$$|\psi_2\rangle + |\psi_3\rangle = \frac{1}{2^{n-1}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |0\rangle$$

$$|\psi_3\rangle = -|\psi_2\rangle + \frac{1}{2^{n-1}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |0\rangle$$

$$|\psi_4\rangle = \mathrm{H}^{\otimes n} |\psi_3\rangle (36.\text{III})$$

$$= -\mathrm{H}^{\otimes n} |\psi_3\rangle + \frac{1}{2^{n-1}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \mathrm{H}^{\otimes n} |0\rangle$$

$$|\psi_4\rangle = -|\psi_1\rangle + \frac{1}{2^{n-1}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle \quad (37.\text{III})$$

$$|\psi_4\rangle = -\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle + \frac{2}{(2^n)^{3/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\sum_{k=0}^{2^n-1}|k\rangle$$

$$|\psi_4\rangle = -u_f|\psi\rangle + \frac{2}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|\psi\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle \qquad N = 2^n$$

$$|\psi\rangle = \frac{1}{\sqrt{N}}[\sum|x\rangle + \sum|y\rangle]$$

↓↓

$$f(x) = 1\ , f(y) = 0$$

$$|A\rangle = \frac{1}{\sqrt{a}}\sum_{x\epsilon \mathrm{A}}|x\rangle \quad (38.\text{III})$$

$f(x) = 1$, كافة العناصر التي هي حل لمشكلة البحث .

$$|B\rangle = \frac{1}{\sqrt{b}}\sum_{x\epsilon \mathrm{B}}|x\rangle (39.\text{III})$$

$f(x) = 0$, كافة العناصر التي ليست حل لمشكلة البحث .

$$|\psi\rangle = \sqrt{\frac{\mathrm{a}}{\mathrm{N}}}|A\rangle + \sqrt{\frac{\mathrm{b}}{\mathrm{N}}}|B\rangle (40.\text{III}) \quad \cos\theta = \sqrt{\frac{\mathrm{a}}{\mathrm{N}}} \qquad ; \sin\theta = \sqrt{\frac{\mathrm{b}}{\mathrm{N}}}$$

$$|\psi\rangle = \cos\theta\,|A\rangle + \sin\theta\,|B\rangle (41.\text{III})$$

نبرهن أن :

$$G|A\rangle = \left(1 - \frac{2a}{\mathrm{N}}\right)|A\rangle - \frac{2\sqrt{ab}}{\mathrm{N}}|B\rangle (42.\text{III})$$

$$G|B\rangle = \frac{2\sqrt{ab}}{\mathrm{N}}|A\rangle - \left(1 - \frac{2b}{\mathrm{N}}\right)|B\rangle (43.\mathrm{III})$$

$$G|A\rangle = \frac{1}{\sqrt{a}}\sum_{x\epsilon \mathrm{A}} \mathrm{G}|x\rangle = -\frac{1}{\sqrt{a}}\sum_{x\epsilon \mathrm{A}} \mathrm{H}^{\otimes n} Z_0 \mathrm{H}^{\otimes n}(-|x\rangle)$$

$$G|A\rangle = -u_f|A\rangle + \frac{2}{\sqrt{2^n}\sqrt{a}}\sum_{x\epsilon \mathrm{A}}(-1)^{f(x)}\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle$$

$$G|A\rangle = |A\rangle + \frac{2}{\sqrt{2^n}}\frac{-a}{\sqrt{a}}\left(\sqrt{\frac{\mathrm{a}}{\mathrm{N}}}|A\rangle + \sqrt{\frac{\mathrm{b}}{\mathrm{N}}}|B\rangle\right)$$

$$G|A\rangle = \left(1 - \frac{2a}{\mathrm{N}}\right)|A\rangle - \frac{2\sqrt{ab}}{\mathrm{N}}|B\rangle$$

$$G|B\rangle = \frac{1}{\sqrt{b}}\sum_{x\epsilon \mathrm{B}} \mathrm{G}|x\rangle = -\frac{1}{\sqrt{b}}\sum_{x\epsilon \mathrm{B}} \mathrm{H}^{\otimes n} Z_0 \mathrm{H}^{\otimes n}(-|x\rangle)$$

$$G|B\rangle = -u_f|B\rangle + \frac{2}{\sqrt{2^n\sqrt{b}}}\sum_{x\epsilon \mathrm{B}}(-1)^{f(x)}\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle$$

$$G|B\rangle = -|B\rangle + \frac{2\sqrt{b}}{\sqrt{N}}\left(\sqrt{\frac{\mathrm{a}}{\mathrm{N}}}|A\rangle + \sqrt{\frac{\mathrm{b}}{\mathrm{N}}}|B\rangle\right)$$

$$G|B\rangle = \frac{2\sqrt{ab}}{\mathrm{N}}|A\rangle - \left(1 - \frac{2b}{\mathrm{N}}\right)|B\rangle$$

في الأساس $\{|A\rangle, |B\rangle\}$

$$G \equiv \begin{pmatrix} 1 - \frac{2a}{\mathrm{N}} & -\frac{2\sqrt{ab}}{\mathrm{N}} \\ \frac{2\sqrt{ab}}{\mathrm{N}} & -\left(1 - \frac{2b}{\mathrm{N}}\right) \end{pmatrix} \equiv \begin{pmatrix} \frac{b-a}{\mathrm{N}} & -\frac{2\sqrt{ab}}{\mathrm{N}} \\ \frac{2\sqrt{ab}}{\mathrm{N}} & \frac{b-a}{\mathrm{N}} \end{pmatrix} (44.\mathrm{III})$$

$$G \equiv \begin{pmatrix} \frac{b-a}{N} & -\frac{2\sqrt{ab}}{N} \\ \frac{2\sqrt{ab}}{N} & -\frac{b-a}{N} \end{pmatrix}\{|A\rangle, |B\rangle\}$$

$$\sin(2\theta) = \frac{2\sqrt{ab}}{\mathrm{N}} \quad , \quad \cos(2\theta) = 1 - \frac{2a}{\mathrm{N}} = \frac{b-a}{\mathrm{N}}$$

$|\psi\rangle = \begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix}$

$$G = \begin{pmatrix}\cos 2\theta & -\sin 2\theta\\ \sin 2\theta & \cos 2\theta\end{pmatrix} (45.\text{III})$$

$$G^k = \begin{pmatrix}\cos(2k\theta) & -\sin(2k\theta)\\ \sin(2k\theta) & \cos(2k\theta)\end{pmatrix} (46.\text{III})$$

وبعد k تحويل ب G

$$G^k|\psi\rangle = \begin{pmatrix}\cos\big((2k+1)\theta\big)\\ \sin\big((2k+1)\theta\big)\end{pmatrix} (47.\text{III})$$

$G^k|\psi\rangle = \cos(2k+1)\theta|B\rangle + \sin(2k+1)\theta\,|A\rangle$

نبحث على عدد المرات التي نطبق فيها G بحيث تنعدم إحدى المركبات

$\cos\big((2k+1)\theta\big) = 0$ K=?

$$G^k|\psi\rangle = \begin{pmatrix}0\\ 1\end{pmatrix} = |B\rangle \quad ; \quad (\text{f(x)} = 0)$$

$$(2k+1)\theta = \frac{\pi}{2} + n\pi$$

لاداعي للتكرار n=0

$$k = \frac{\pi}{4\theta} - \frac{1}{2} + \frac{n\pi}{2\theta} \qquad ; k\epsilon\mathbb{N} \qquad ; \ \text{k} = 1,2,3, \dots \dots$$

$\theta = \arcsin\left(\sqrt{\frac{a}{N}}\right)$ a: nombre $|x\rangle, \text{f(x)} = 1$

لاندري عدد العناصر x بحيث $\text{f(x)} = 1$

a مجهول

عمليا نعلم أن a<< N

a =1

$$\theta \approx \frac{1}{\sqrt{N}}$$

$$k = \frac{\pi\sqrt{N}}{4} - \frac{1}{2} + \frac{n\pi}{2\theta}$$

n=0 $k = \frac{\pi\sqrt{N}}{4} - \frac{1}{2}$

الطرف الصحيح $k \equiv [\frac{\pi\sqrt{N}}{4}]$

مثلا : لو نعلم أن عدد العناصر التي $f(x) = 1$ صغير, إذا نكرر Grover حوالي $k = \frac{\pi\sqrt{N}}{4}$

احتمال القياس على الحالة $G^k|\psi\rangle \rightarrow |\sin((2k+1)\theta)|^2 = p$

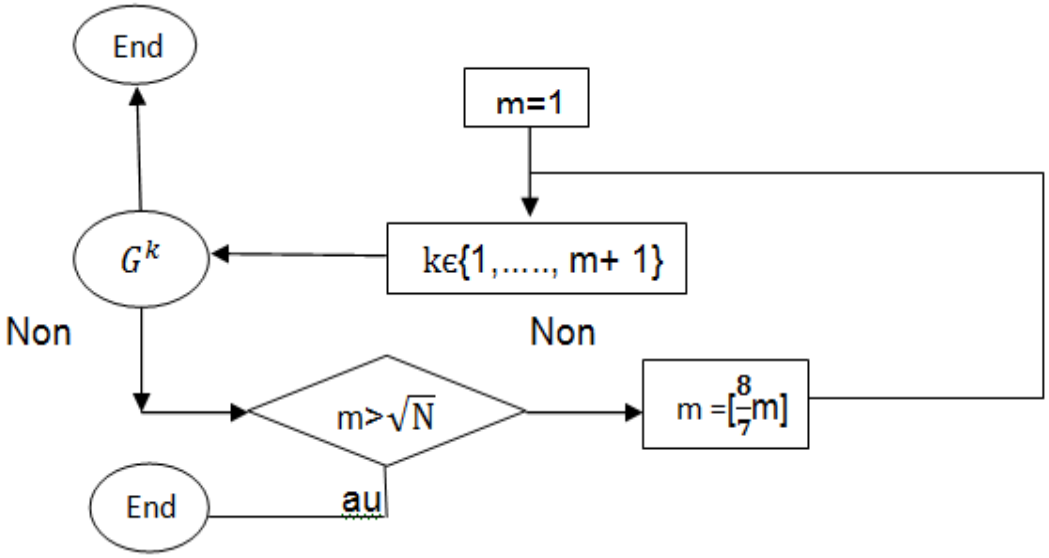
وتكون نتيجة القياس $|B\rangle$

$$p = |\operatorname{Sin}\left(\left(\frac{\pi\sqrt{N}}{2} + 1\right)\frac{1}{\sqrt{N}}\right)|^2 = |\operatorname{Sin}\left(\frac{\pi}{2} + \frac{1}{\sqrt{N}}\right)|^2 = cos^2(\frac{1}{\sqrt{N}}) \approx 1$$

الحالة العامة N a<< ليس صغير أمام N

لا نطبق مباشرة Grover

نقوم بالخطوات التالية حيث نستعمل Groverk مرة



رسم تخطيطي (III. 7) يوضح Grover kمرة

III .4.4. خطوات خوارزمية *Grover*

1) X register nqbit|0000 0⟩
الحالة الإبتدائية ل X هي $|0^n\rangle$

2) نطبق على X التحويل : $GXG = -H^{\otimes n}Z_0H^{\otimes n}Z_f$; , k مرة

3) نقيس X

التحليل : $-Z_f$, $H^{\otimes n}Z_0H^{\otimes n}$

↓↓

reflexionreflexion

ليكن

الفئة الصحيحة $A = \{x \in \{0,1\}^n; f(x) = 1\}$

الخاطئةالفئة $B = \{x \in \{0,1\}^n; f(x) = 0\}$

عدد العناصر a=|A| , b=|B|

$$N = 2^n|\psi\rangle = \frac{1}{\sqrt{N}}[\sum|x\rangle + \sum|y\rangle]$$

$$f(x) = 1 \quad , \quad f(y) = 0$$

نعرف

$$|A\rangle = \frac{1}{\sqrt{a}}\sum_{x\epsilon A}|x\rangle \qquad ; \qquad f(x) = 1$$

$$f(x) = 0; |B\rangle = \frac{1}{\sqrt{b}}\sum_{x\epsilon B}|x\rangle$$

بعد التحويل $H^{\otimes n}$: حيث $|\psi\rangle = H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\epsilon\{0,1\}^n}|x\rangle\,|0^n\rangle$

$$|\psi\rangle = \sqrt{\frac{a}{N}}|A\rangle + \sqrt{\frac{b}{N}}|B\rangle$$

$$\rightarrow \text{rotation} \qquad \theta = \text{Arcsin}\, 2\sqrt{\frac{ab}{N}}$$

بعد المرحلة الأولى يصبح السجل $|\psi\rangle = \cos\theta\,|B\rangle + \sin\theta\,|A\rangle$

نضع $(2k+1)\theta \approx \frac{\Pi}{2} \leftarrow k \approx \frac{\Pi}{4\theta} - \frac{1}{2}$

عندما a=1

$$\Theta = \text{Arcsin}\sqrt{\frac{1}{N}} \approx 1/\sqrt{N} \rightarrow k = [\frac{\Pi}{4}\sqrt{N}]$$

$$X = |0^n\rangle \qquad \rightarrow K \text{ fois} \quad \rightarrow |A\rangle$$

إحتمال أن تكون نتيجة القياس x الذي $f(x) = 1$

$$P = sin^2(\left(2\left[\frac{\Pi\sqrt{N}}{4}\right] + 1\right) Arcsin\left(\frac{1}{\sqrt{N}}\right))$$

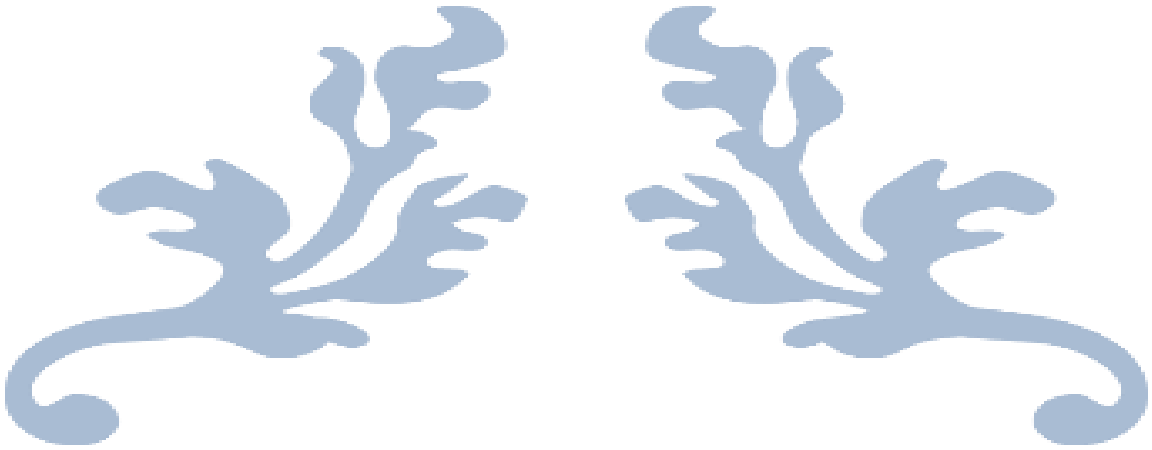
$$p \rightarrow 1$$

$$N \rightarrow \infty (N \approx 16)$$

و في الحالة العامة $a\neq 1$ يصبح من الصعب تحديد عدد تكرارات Grover لذى نقوم بتكرار Gكما موضح في الرسم التخطيطي (III. 7) حسب الخوارزمية التالية

1)m =1
2)choose kϵ{1,.....,1 m+} run Grover k time if x find then halt.

m3) if>$\sqrt{N}$ then fail Else m= [$\frac{8}{7}$m] and goto 2.



الخاتمة العامة

الخاتمة العامة

من المنتظر أن يشهد العالم قفزة هائلة في مجال الاتصالات والمعلوماتية، تقوم بها ميكانيك الكم وترسم مسارها نظرية المعلومات الكمية. حجر الزاوية الذي تعتمد عليه الحوسبة الكمية هو الخوارزميات الكمومية.

الخوارزميات الكمومية تختزل العمليات الكلاسيكية لأنها تعتمد على الظواهر الكمومية من التداخل والتشابكالكمي. والذي قد يصبح هو الأداة التي يتم بها الاتصال اليومي في عالمنا غدا، قد يصبح كل الخيال العلمي الذي حسبناه يوما ما مستحيلا واقعا ملموسا، لكن غدا البعيد هذا يقترب بالسرعة التي يتم فيها فهم الحوسبة الكمومية والتحكم به.

فالحاسوب الكمي هو خوارزمية تنفرد بها ميكانيك الكم. حيث يعتمد على النظم الكمية لتحويل بتات كمومية إلى نتائج على شكل بتات كمومية يتم قياسها لقراءة النتائج.

لايجب أن تتفاعل الجملة الكمومية مع الخارج، سيصبح بمثابة جهاز قياس وهكذا تتلاشى التصرفات الكمومية(Decoherence).

بالعمل على هذه المذكرة تعلمنا الحوسبة الكمومية وتمكنا من طريقة العمل في هذا المجال. نطمح أن هذا الموضوع سيفتح لنا أبوابا ومشاريع بحثية نستطيع من خلالها المشاركة في هذه النقلة النوعية المرتقبة.

المراجع

قائمة المراجع

[1] **Michael A. Nielsen, Isaac L. Chuang-Quantum , Quantum Computation and Quantum Information,**AmericaUniversityPress ,New York (2010).

[2] Jürgen Audretsch, Entangled Systems : New Directions In Quantum Physics, Wiley, Weinheim (2007).

[3] Lingxiao Zhang, Engineering Exchange Interaction in Coupled Spin-qubit Quantum Dots, A doctoral dissertation, university of Illinois at UrbanaChampaign, United States of America (2008).

[4] **CSE 599d - Quantum Computing "One Qubit, Two Qubit",**Dave Bacon, *Department of Computer Science & Engineering, University of Washingtom*

[5] Exploration in quantum computing .C.P2011.xxII.717.P.Hardcover

ISBN :978-1184628-886-9.

[6] **CSE 599d - Quantum ComputingReversibleClassical Circuits and the Deutsch-JozsaAlgorithm.**

Dave Bacon Department of Computer Science & Engineering, University of Washington.

[7] IngemarBengtsson and Karol Zyczkowski, Geometry Of Quantum States An Introduction to Quantum Entanglement, Cambridge University Press, New York (2006).

[8] AlisaBokulich and Gregg Jaeger, Philosophy Of Quantum Information And Entanglement, Cambridge University Press, Cambridge (2010).

[9] AnirbanPathak, Elements Of Quantum Computation And Quantum Communication, Taylor & Francis Group, Florida (2013).

[10] SàndorImre and F. Balàzs, Quantum Computing and Communications : An Engineering Approach, Wiley, Germany (2005).

[11] Giuliano Benenti, Giulio Casati and Giuliano Strini, Principles Of Quantum Computation And Information, Volume I, World Scientific Publishing, Singapore (2005).

[12] A.F.J.Levi, Applied Quantum Mechanics, Second Edition, Cambridge University Press, United States of America (2006).

[13] W. K. Wootters and W. H. Zurek, A single quantum cannotbecloned, Nature, vol. 299 (1982).

[14] EmmanuelDesurvire, Classical and Quantum Information Theory : AnIntroduction for the Telecom Scientist, Cambridge University Press, United States of Am erica (2009).

[15] Marvin V. Zelkowitz, Advances in Computers, volume 56, Academic Press, Great Britain (2002).

[16] JhonPreskill , Lectures Notes on Quantum Information Theory.

[http://www.theory.caltech.edu/people/preskill/ph229/].

[17] Stephen M. Barnett, Quantum Information, Oxford University Press, United States Of America (2009).

[18] Benjamin Schumacher and Michael D. Westmoreland, Quantum Processes,Systems, and Information, Cambridge University Press, United States ofAmerica (2010).

[19] **CSE 599d - Quantum ComputingReversible Classical Circuits and the Deutsch-Jozsa Algorithm.**

Dave Bacon Department of Computer Science & Engineering, University of Washington.

[20] **CSE 599d - Quantum Computing Simon's Algorithm**

Dave Bacon Department of Computer Science & Engineering, University of Washington.

الملخص:

الحاسوب الكلاسيكي هو خوارزمية تحول بتات مخزنة على شكل نظام ثنائي (0,1) إلى نتائج كذلك على شكل بتات . أما الحاسوب الكمومي هو خوارزمية تعتمد على النظم الكمية لتحويل بتات كمومية إلى نتائج على شكل بتات كمومية يتم قياسها لقراءة النتائج . الخوارزميات الكمومية تختزل العمليات الكلاسيكية لأنها تعتمد على الظواهر الكمومية من التداخل والتشابك من أهم هذه الخوارزميات هي خوارزمية Grover التي تسمح بفصل المعطيات حسب معيار معين تفوق بطريقة أسية الخوارزميات الكلاسيكية. تناولت هذه المذكرة موضوع الحاسوب الكمومي، فحددت الخوارزميات التي تصف عمل الحاسوب الكمي إضافة إلى Grover تطرقنا لخوارزمية Simon وخوارزمية Deutsch–Jozsa، وتم فيها القيام بالعمليات والبوابات الكمومية، أين تم التعرض للتشابك الكمي، ومن تطبيقاته تعرضنا لنظرية عدم الاستنساخ والنقل الكمي والترميز المكثف وتوزيع المفتاح الكمومي.

الكلمات المفتاحية : التشابك، التراكب، الكمبيوتر الكمي، البت الكمي(qubit)، خوارزمية، البوابات الكمومية

Abstract :

The classical computer is an algorithm that transforms bits stored in a binary form into results that are like wise bits. Similarly, the quantum computer is an algorithm based on quantum laws, which transforms qubits into other yielding the aleshed results after measuring. Quantum algorithms reduce the classic operations because of the phenomen of entanglement and interference. One important example is Grover's algorithm,allows separating elates (according to some criterion) in a time exponentially less than that of the classic algorithms. This dissertation treats the above subject. We focus on some examples that exemplify hour a quantum computer might work. The main algorithms treated here are the ones clue to Grover, Simon, Deutch-Jozsa. As an application we touched on the theory" no-Cloning Theorem", "quantum teleportation" and 'dense cryptography' and 'Quantum KeyDistribution'.

Key words: Entanglement, interference, quantum computer, qubit, algorithm, quantum gates.